*IOSR Journal of Engineering (IOSRJEN)*
*e-ISSN: 2250-3021, p-ISSN: 2278-8719, www.iosrjen.org*
*Volume 2, Issue 9 (September 2012), PP 42-49*

# High Quality Monitoring with Location Anonymization for WSN

RAGHAVENDRA.M[1], Dr.D.KAVITHA[2]
[1]*Department of CSE, G.Pullareddy Engineering College,Kurnool, Andhra Pradesh, India*
[2]*Department of CSE, G.Pullareddy Engineering College,Kurnool, Andhra Pradesh, India*
*Associate Professor*

***Abstract***—*Due to technological advances in sensor technologies, Wireless Sensor Networks are widely used for location monitoring. In such systems monitoring personal locations is done through Internet server. As the server is untrusted, it may cause threats pertaining to privacy of individuals being monitored. This is the potential risk to be addressed. This paper presents two algorithms to address this problem. These algorithms achieve two purposes. The first one is that they can improve quality of monitoring locations while the second one is for location anonymization so as to preserving personal location privacy. The first algorithm is resource – aware which is aimed at reducing computational and communicational cost while the quality – aware algorithm is aimed at improving the quality of monitoring locations. Both are having a feature that preserves personal location privacy. The system is evaluated with simulation experiments using NS2. The empirical results revealed that the proposed system can provide high quality monitoring besides preserving personal location privacy.*

***Index Terms***— *WSN, privacy preservation, location monitoring*

## I. INTRODUCTION

The technological innovations in sensor technologies paved way for Wireless Sensor Networks to be used many applications for both civilian and military purposes. Location monitoring and surveillance are also part of these applications. The location monitoring systems are implemented by using two kinds of sensors. They are counting sensor and identity sensor. The identity sensors are meant for pinpointing exact location of persons in given location while the count sensors are meant for reporting the number of persons present in the given location. Identity sensors examples are in [1] and [2] while counting sensors examples are described in [3], [4] and [5].

Monitoring personal locations required a server being used for location query processing. The server is essentially an Internet server and therefore it is untrusted. Such server may cause potential risk to the privacy of individuals being monitored. This is because hackers might be able to get sensitive personal information through compromised server [2], [6], [7], [8]. The identity sensors especially provide exact location of individuals being monitored which causes privacy breaches when hacked from server. The counting sensors also provide information related to count of people being monitored. It also breaches privacy when hacked by adversaries. In papers [8] and [9] solution is provided for such problems by introducing the concept of aggregating location information and removing identities from such information [8], [9].

This paper proposes a system for location monitoring that ensures anonymity with respect to privacy of individuals being monitored and also improves quality of sensing or location monitoring. K-anonymity concept is used in the proposed system in order to avoid distinguishing an individual among a group of people monitored though such information is hacked. For both identity and counting sensors, the same solution is adopted and k-anonymity concept is used. Aggregation of location details is capable of removing actual individuals' sensitive data. With the help of this the proposed system is capable of providing high quality in location monitoring and also efficiency in working and preserving personal location privacy. The proposed system is capable of avoiding privacy leakage with efficient algorithms and high quality location services. The adversaries can't get actual sensitive information even when they are able to hack server due to the location aggregation and k-anonymity concept used in the proposed system.

The system is capable of knowing aggregate information pertaining to location of individuals being monitored; it can also provide such services though a query system. For instance our query system can provide number of individuals being monitored by sensors. Spatial histogram concept is used to achieve this. The proposed system uses two novel algorithms known as quality – aware algorithm and resource – aware algorithm. The first algorithm is meant for improving quality of location monitoring services with in terms of accuracy. The second algorithm is meant for improving the efficiency in usage of computational power and communications. However, both are aware of preserving personal location privacy. The system is evaluated

using simulations made using NS2. The simulation results reveal that our system is able to preserve privacy of individuals being monitored by sensors of WSN. At the same time it has improved the quality of monitoring services dramatically.

## II. RELATED WORK

In [10] and [11], the privacy enforcement by using privacy policies is described. It is a straight format approach which makes use of location information collected by sensors [10], [11] and perform something anonymization of stored data before providing it to any one through queries [12]. These approaches have some drawback that is they fail to prevent internal thefts of data and disclosure of it illegally. Location anonymization is the recent phenomenon which ensures that location information is secured and thus privacy of personal location is preserved. Such techniques are used to avoid security breaches in location monitoring services and systems. However, these techniques are making use of one of the following three concepts. The first one is known as false locations which indicate that sensors might send many locations out of which there may be only one correct location [13]. The second one is spatial cloaking which converts user's locations into a clocked spatial area that ensure to satisfy security requirements as discussed in [14], [15], [16], [17], [18], [19], [20], [21], [22], [23]. The third one is space transformation which is meant for converting location based results of queries into another space by using some encoding in spatial information [24]. Out of these concepts, our problem can only be solved using the spatial clocking technique. The rationale behind this is that the other two are not suitable to our problem as the first one provides false location information while the third one is transforming the space which has trade-offs between quality services and privacy preserving. The spatial clocking is the technique is capable of providing aggregate location information to the underlying server. It also achieves balance between the privacy requirements and also quality of services. Its main privacy requirements include k-anonymity [12], [22].

In case of architecture of the system, there are three classifications. Systems based on spatial cloaking techniques [14], [15], [17], [20], [21], [22], [23], systems based on the distributed techniques [18], [19], and systems based on peer-to-peer [16] approaches. Out of them the problem with the centralized approach is the fact that it can't prevent internal attacks. The distributed systems are different from the wireless sensor networks and therefore the distributed approaches are not suitable for the present paper. Peer to peer can be applied but previous research showed that it is not good approach it can hide only one identity. Therefore for WSN spatial cloaking techniques spares well and practically suitable. Cricket [2] is the only existing system in terms of privacy preserving and location monitoring services. However it provides such services in decentralized systems. In this system users are capable of letting whether their location information can be disclosed or not. When compared to our system, it is in contrast as our system is aimed at providing aggregate location information of all people monitored by sensors. The work that has close resemblance with our work is the algorithm described in [6] which partitions space of the system into some units. The system rounds the count of people for security reasons. This approach is not suitable for environments such as shopping mall, outdoor environments etc. The proposed system in this paper has differences from this as no hierarchical structure is used and utilization of anonymity is our system.

## III. SYSTEM MODEL

The outline of architecture of proposed system is as shown in fig. 1. A WSN is considered with many sensor nodes covering certain area. The sensor nodes are integrated with a server which can save the data sent by sensors permanently. There are moving objects that come into the purview of each sensor. The job of sensors is to send location information of the objects that they detect. This information is stored in server. The server gives k-anonymity privacy requirement to sensor network and the sensors provide aggregate locations information to the server in turn. Thus the server stores aggregate location information which is built in such a way that it can't disclose individual's personal location privacy.

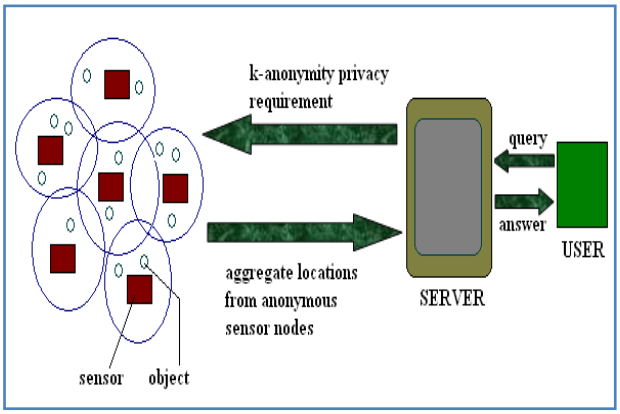



Fig. 1: Block diagram of proposed system architecture

When user requests server for location information by raising a query, the server takes it gives information to user. This is the proposed system architecture. In order to make this system to achieve location anonymity and high quality in location services, two algorithms are proposed. They are known as resource-aware algorithm and quality – aware algorithm.

## IV. LOCATION ANONYMIZATION ALGORITHMS

The proposed location anonymization algorithms are meant for achieving three purposes. The first purpose is that they can enhance the quality of location services. The second purpose is to minimize the computational resources and communication overhead. The third purpose of them is to ensure anonymity of personal location privacy.

**Resource – Aware Algorithm**

This algorithm is meant for improving resource consumption. It minimizes the computational cost and communication cost while preserving the personal location privacy. The algorithm out line is given in fig. 2.

**Algorithm 1 Resurce aware**

1: function RESOUCEAWARE (Integer k, Sensor m, List R)
2. PeerList ← {φ} // Step 1: The broadcast step
3. Send a message with m's identity m. I.D, sensing area m.Area, and object Count m, Count to m's neighbor peers
4. If receive a message from Peer p, i.e.,(p.ID,p.Area,p.Count) then
5. Add the message to Peer List
6. if m has found the adequate number of objects then
7. Send a notification message to m's neighbors
8. end if
9. if some m's neighbor has not found an adequate number of objects then
10. forward the message to m's neighbor
11. end if
12. end if //setup 2: the cloaked area step
13. S ← {m}.
14 Compute a score for each peer in PeerList.
15. Repeatedly select the peer with the highest score from PeerList to S until the total number of objects in S at least k
16. Area ← a minimum bounding rectangle of the sensor nodes in S
17. N ← the total number of objects in S // Step 3: The validation step
18. if No containment relationship with Area and R ε R then
19. Send(Area,N) to the peers within Area and the server
20 . else if m's sensing area is contained by some R ε R then
21. Randomly select a R' ε R such that R'. Area contains m's sensing area.
22. Send R' to the peers within R'. Area and the server
23. else
24. Send Area with a cloaked N to the peers within Area and the Server.
25. end if.

Fig. 2: Outline of resource – aware algorithm

The resource aware algorithm has three major steps. The first step is known as the broadcast step. In order to minimize the communication and computational cost, this step is aimed at informing all sensor nodes to know required number of objects to be considered in a cloaked area. In the first steps a sensor node sends its ID, sensing area and other details as given in the algorithm to all other sensor nodes. If a sensor receive a message it adds that node in the peer list and sends a message to its neighbors if the node has adequate number of objects. The step2 is cloaked area step in which each sensor node blurs its sensing area into an area known as cloaked area with k objects and k-anonymity is achieved. In order to reduce computational cost, this step also uses a greedy approach. The third step is known as validation step in which it avoids reporting aggregate relationships. Therefore adversaries can't get any information which breaches privacy.

**Quality – Aware Algorithm**

This algorithm is meant for improving quality of location services. Besides this, it also takes care of location anonymity. The outline of this algorithm is given in fig. 3.

**Algorithm 2 Quality aware location anonymization**

1. function QUALITYAWARE (Integer k, sensor m, Set init_solution,List R)
2. current_min_cloaked_area ←init_solution // Step 1: The search space step
3. Determine a search space S based on init_solution
4. Collect the information of the peers located in S //Step 2: The minimal cloaked area step
5. Add each peer located in S to C[1] as an item
6. Add m to each itemset in C[1] as the first item
7. for i=1; i≤4;i++ do
8. for each itemset X= {a1,.....,aδ+1 } in C[i] do
9. if Area (MBR(X)) < Area (current_min_cloaked_area) then
10. if N(MBR(X))≥ k then
11. current_min_cloaked_area ←{X}
12. Remove X from C[i]
13. end if
14. else
15. Remove X from C[i]
16. end if
17. end for
18. if i<4 then
19. for each itemset pair X = {x1,....xδ+1}, Y = {y1,.....,yδ+1} in C[i]do
20. if x1 = y1,.....,xδ = yδ and xδ+1 ≠ yδ+1 then
21. Add an itemset {x1,.....,xδ+1,yδ+1} to C[i+1]
22. end if
23. end for
24. end if
25. end for
26. Area ←a minimum bounding rectangle of current_min_cloaked_area
27. N ←the total number of objects in current_min_cloaked_area // Step 3: The validation step
28. Lines 18 to 25 in Algorithm 1

Fig. 3: Quality – aware algorithm

As can be seen in fig. 3, this algorithm has three steps. The first step is known as the search space step. The second step is named the minimal cloaked area step while the third step is known as the validation step. The first step is meant for finding the search space. This is required to reduce communication and computational cost. The step 2 takes a collection of peers that live in the search space "S". They are taken as input and computation takes place to find minimum cloaked area for the given sensor. Although search space is pruned for efficiency, all combinations are to be searched. To overcome this problem, two optimization techniques are introduced. The first optimization technique is to verify only four nodes almost instead of all combinations. The other optimization technique has two properties namely monotonicity property and lattice structure. Lattice set

is generated to improve search operations while monotonicity is used to reduce the number of objects in the MBR. Afterwards, a progressive refinement is performed for finding minimal cloaked area.

## V. SPATIAL HISTOGRAM

In this paper, we also develop a spatial histogram which is meant for estimating the distribution of monitored objects. It runs in the server machine and it functionality is based on the aggregate locations. It is implemented as a two – dimensional array. The algorithm used to build spatial histogram and maintaining it is outlined in fig. 4.

**Algorithm 3 Spatial histogram maintenance**

1. **Function HISTOGRAMMAINTENANCE(AggregateLocationSet R)**
2. **for each aggregate location Rε R do**

**if there is an existing partition P = {$R_1$,…..,$R_{|P|}$} such that R.Area ∩ $R_k$.Area = θ for every $R_k$ ε P then**

4. **add R to P**
5. **else**
6. **create a new partition for R**
7. **end if**
8. **end for**
9. **for each partition P do**
10. **for each aggregate location $R_k$ε P do**
11. **$R_k$.N← $\sum_{G(i,j)\varepsilon Rk.Area}$ H(i,j)**

**for every cell G(i,j) ε $R_k$.Area, H[i,j]← $\underline{R_k.N}$ No. of cells within $R_k$.Area**

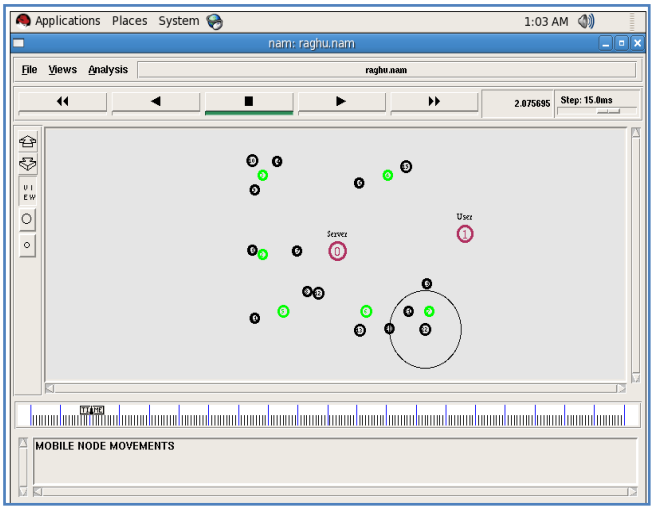
12. **end for**
13. **P.Area ← $R_1$.Area U…..U $R_{|P|}$.Area**
14. **For every cell G(i,j) !ε P.Area,**
    **H[i,j] = H[i,j] + $\sum_{Rk\varepsilon P} \underline{R_k.N\text{-}R_k.N}$ No.of cells outside P.Area**
15. **end for**

Fig:4 Spatial histogram maintenance algorithm

As can be seen in fig. 4, the algorithm outlines the histogram creation and maintenance algorithm that is meant for estimating the distribution of monitored objects.

## VI. IMPLEMENTATION

The proposed architectural model and algorithms have been implemented in NS2 that runs in Linux OS. The NS2 implementation of simulation is shown in figures 5, 6, and 7.




As can be seen in fig. 5, the simulation shows sensor nodes, people or objects in movement, user and server. It only shows the movement of sensor nodes and also objects in motion.

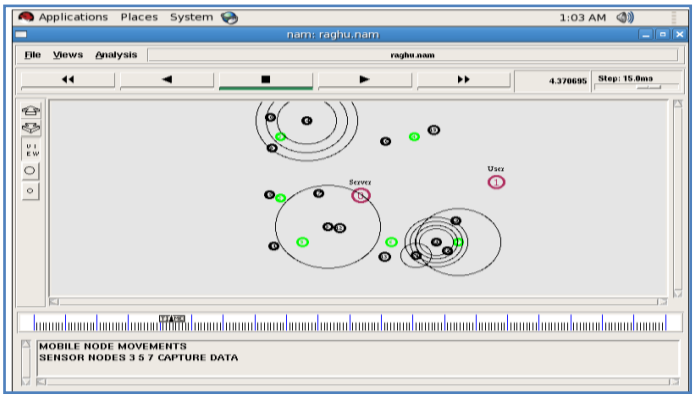



Fig. 6: shows sensor nodes 3, 5 and 7 capturing data and sending to server

As can be viewed in the simulation shown in fig. 6, the nodes 3, 5, and 7 are capturing data pertaining to moving objects or people. In the simulation nodes are having their sensing areas marked besides having the user and server represented in the simulation.

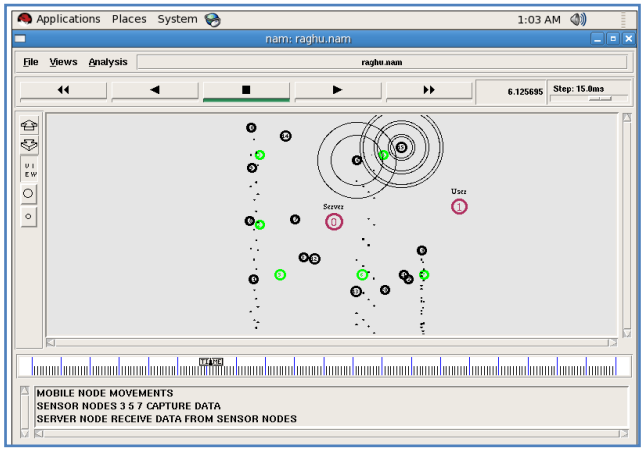



Fig. 7 shows the further simulation of the WSN

As can be viewed in fig. 7, the simulation shows further communication between sensor nodes and the server. The resource-aware and quality-aware algorithms are in place. The system is able to demonstrate the proposed architectural model.

## VII. EXPERIMENTAL RESULTS

The experiments made with the simulations using quality – aware and resource – aware algorithms revealed that they are capable of minimizing computational cost and communication cost. At the same time they are able to preserving personal location privacy.

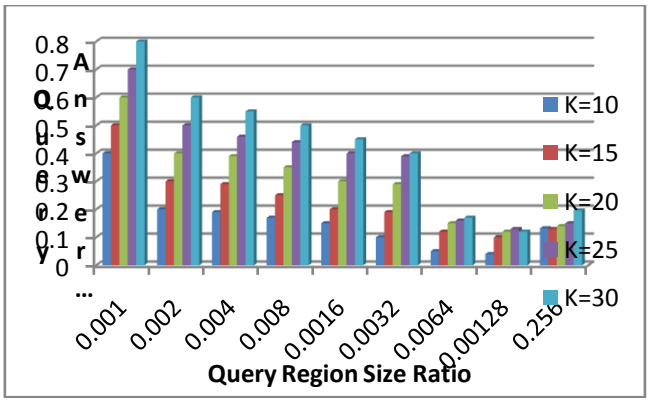



Fig. 8: Resource – aware algorithm

As can be seen in fig. 8, the resource aware algorithm performance is presented. As it is evident in the graph, the more query region size ratio, the less is query answer error. It ensures less computational cost and communication cost.

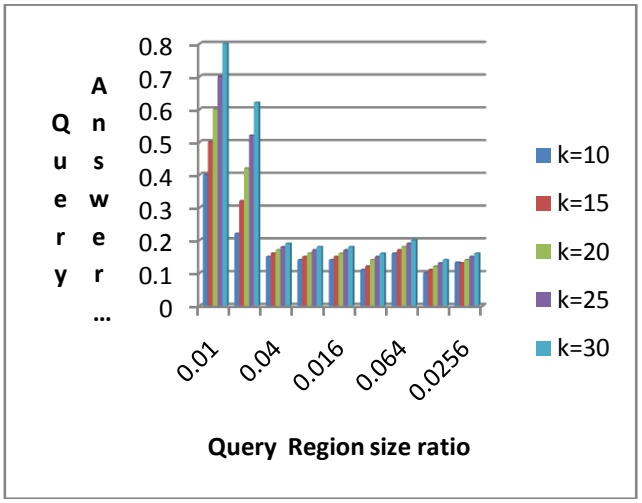



**Fig. 9: Quality – aware algorithm**

As can be seen in fig. 9, the quality aware algorithm performance is presented. As it is evident in the graph, the more query region size ratio, the less is query answer error. It ensures that the quality of the results is improved.

## VIII. CONCLUSIONS

The system presented in this paper is pertaining to WSN and its privacy preserving of the objects being monitored by sensors. To achieve this two algorithms are implemented. They are known as resource – aware privacy preserving algorithm and quality – aware privacy preserving algorithm. The first algorithm ensures that fewer resources are consumed and minimizes the cost of communication and computation. The second algorithm is meant for improving quality of location services. However, both the algorithms are having the feature of privacy preserving. K-anonymity concept is used to have aggregate location information which forms a clocked area. This kind of information is without sensitive personal identity in the available location related information. Thus the adversaries can't get sensitive information even if they hack the information from server. The empirical results revealed that the proposed algorithms are working as expected and they can be used in the real world WSN applications.

## REFERENCES

[1] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, .The anatomy of a context-aware application,. in *Proc. of MobiCom*, 1999.
[2] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, .The cricket location-support system,. in *Proc. of MobiCom*, 2000.
[3] B. Son, S. Shin, J. Kim, and Y. Her, .Implementation of the realtime people counting system using wireless sensor networks,. *IJMUE*, vol. 2, no. 2, pp. 63.80, 2007.
[4] OnesystemsTechnologies, .Counting people in buildings. http://www.onesystemstech.com.sg/index.php?option=com content&task=view%&id=10..
[5] Traf-Sys Inc., .People counting systems. http://www.trafsys.com/products/people-counters/thermal-sensor.aspx..
[6] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald,.Privacy-aware location sensor networks,. in *Proc. of HotOS*, 2003.
[7] G. Kaupins and R. Minch, .Legal and ethical implications ofemployee location monitoring,. in *Proc. of HICSS*, 2005.
[8] Location Privacy Protection Act of 2001, http://www. techlawjournal.com/cong107/privacy/location/s1164is.asp..
[9] Title 47 United States Code Section 222 (h) (2), http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname =browseusc&do%cid=Cite:+47USC222..
[10] K. Bohrer, S. Levy, X. Liu, and E. Schonberg, .Individualized privacy policy based access control,. in *Proc. of ICEC*, 2003.
[11] E. Snekkenes, .Concepts for personal location privacy policies,.in *Proc. of ACM EC*, 2001.
[12] L. Sweeney, .Achieving k-anonymity privacy protection using eneralization and suppression,. *IJUFKS*, vol. 10, no. 5, pp. 571.588, 2002.

[13] H. Kido, Y. Yanagisawa, and T. Satoh, .An anonymous communication technique using dummies for location-based services,. in*Proc. of ICPS*, 2005.
[14] B. Bamba, L. Liu, P. Pesti, and T. Wang, .Supporting anonymous location queries in mobile environments with privacygrid,. In *Proc. of WWW*, 2008.
[15] C. Bettini, S. Mascetti, X. S. Wang, and S. Jajodia, .Anonymity in location-based services: Towards a general framework,. in *Proc. of MDM*, 2007.
[16] C.-Y. Chow, M. F. Mokbel, and X. Liu, .A peer-to-peer spatial cloaking algorithm for anonymous location-based services,. In *Proc. of ACM GIS*, 2006. X
[17] B. Gedik and L. Liu, .Protecting location privacy with personalized k-anonymity: Architecture and algorithms,. *IEEE TMC*, vol. 7, no. 1, pp. 1.18, 2008.
[18] G. Ghinita, P. Kalnis, and S. Skiadopoulos, .PRIV ´ E: Anonymous location-based queries in distributed mobile systems,. in *Proc. Of WWW*, 2007.
[19] G. Ghinita1, P. Kalnis, and S. Skiadopoulos, .MobiHide: A mobile peer-to-peer system for anonymous location-based queries,. In *Proc. of SSTD*, 2007.
[20] M. Gruteser and D. Grunwald, .Anonymous usage of locationbased services through spatial and temporal cloaking,. in *Proc. Of MobiSys*, 2003.
[21] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, .Preventing location-based identity inference in anonymous spatial queries,. *IEEE TKDE*, vol. 19, no. 12, pp. 1719.1733, 2007.
[22] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, .The New Casper: Query procesing for location services without compromising privacy, . in *Proc. of VLDB*, 2006.
[23] T. Xu and Y. Cai, .Exploring historical location data for anonymity preservation in location-based services,. in *Proc. of Infocom*, 2008.
[24] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, .Private queries in location based services: Anonymizers are not necessary,. in *Proc. of SIGMOD*, 2008.