# QUALITY-AWARE LOCATION MONITORING FOR WIRELESS SENSOR NETWORKS

M.B.Raghavendra[1] and Dr. P.Harini[2]

[1]II year M.Tech(CSE), JNTUK, St.Ann'sCollege of Engineering &Technology, Chirala
mbraghav@gmail.com
[2]HOD-CSE, JNTUK, St. Ann's College of Engineering &Technology, Chirala
hpogadadanda@yahoo.co.in

***ABSTRACT***

*Surveillance of personal locations with an untrusted system causes privacy breach/threats to the individuals those who are monitored. At this point, we propose a quality-aware locality monitoring system for wireless sensor networks. In this system, we outline a couple of in-network location algorithms such as resource-aware and quality aware algorithms, aimed to provide high-end location monitoring services for system users with outstanding quality, while protecting personal location privacy. Two techniques are based on the well-established (K) anonymity privacy concept; i.e., a person is unique among (K) individuals, to enable trusted sensor nodes to provide the average location information of monitored objects of the system. Each compound location is a part of a surveyed area/ location (L) along with the number of surveyed objects residing in (L), where (L) contains at least (K) persons. The resource aware algorithm minimizes communication cost and computational cost, while the quality aware algorithm maximizes the correctness of the aggregate location by lowering their monitored regions. To use the location information, to provide location monitoring service, we use a spatial histogram method, which calculates the distribution of the monitored objects created on the collected aggregate location information. Then, the calculated distribution provides location monitoring services by answering a series of questions. The system is evaluated through virtual experiments. The results indicate that this system provides an excellent location monitoring services while ensuring location privacy of the monitored persons.*

***KEYWORDS***

Quality Aware, wireless sensor networks, Resource Aware, spatial histogram

## 1. INTRODUCTION

The advance wireless sensor technologies gave rise to numerous applications widely used by general citizens as well as in military operations. The applications based on the information of personal locations such as the surveillance and location systems are recognized as counting sensors or identity sensors.

In an identity sensor, every individual carries a signal sender/receiver unit with a unique public identifier. Exact indication of location of each monitored person is possible with identity sensors. Whereas, counting sensor like the photo electric sensor and thermal sensors are installed to report the number of persons in that sensing areas. However, monitoring personal locations with an untrusted system may cause privacy threats to the monitored individuals. This may aid in utilization of the location information, gathered by the system, to deduce personal information.

DOI : 10.5121/ijasuc.2012.3409 

The sensor nodes in the identity sensors report the precise location information of monitored objects. Thus, using identity sensors proximately poses a significant privacy breach. The concept of aggregate location information has been developed to challenge the privacy breach in identity sensors. Aggregate location information is a collection of location data related to a category or a group from which individual identities have been removed. This is a fair method to protect location privacy. As though the counting sensor provides aggregate location info, they also possess privacy breaches.

Here, assume that there are 11 counting sensor nodes installed in 9 different rooms R1 to R9, including two hall ways C1 and C2 in Fig. 1a. The non-zero no. of objects detected by each sensor node is depicted as a no. in the braces. Figure 1b and 1c provide the figures reported by the same sensor nodes at two consecutive times T1 and T2 respectively. If R3 is Andrew's office room, an adversary knows Andrew is in room R3 at time T1. Then, the rival knows that Andrew left R3 at time T1 and left to C2. This can be deduced by referring to the no. of objects detected by sensor nodes in the room, R3 and hall, C2. Likewise, we can infer that Andrew left C2 at time T2 and left to R7.

Such information leakage may result in several privacy breaches. Knowing that a person has visited certain health rooms may know the entire activity in that building or location. Also, detecting that a person has stayed at a hotel may reveal confidential information.

This paper proposes a quality-aware location monitoring system for wireless sensor networks that provide excellent and privacy controlled monitoring services. The system is based on the well-established privacy concept K-anonymity that states each person is indistinguishable among (K) persons. In this system, each sensor node shadows its exact sensing areas into a cloaked area, where (K) persons are present. Aggregate location information is reported by each sensor node, which is in a cloaked area (A) with the no. of objects (N) located in the cloaked areas, so that each cloaked area (A) contains at least (K) persons, then (N), (K) is reported to the server. It is essential to record the value of (K) achieves a transaction between the severity of privacy and the quality of location monitoring services. A smaller (K) indicates less privacy protection as a smaller cloaked region will be reported by the sensor node. This ensures a better monitoring service. However, a larger (K) results in a larger area will reduce the quality of location monitoring services, but it ensures better protection of privacy. Our system can avoid the privacy leakage as shown in Fig. 1

Providing poor location monitoring services especially for small areas may allow rivals to track users. So, we provide high quality services for larger regions. The classification of a low region is relative to essential anonymity, because this system provides better services for this same area if we minimize the required levels of anonymity. Thus, a rival cannot conclude the number of objects currently present in a small region from our system output. Hence, the rival can't know that Andrew is in R3.

Now, to avoid this situation, we propose two algorithms: namely resource aware and quality aware algorithms. Both these algorithms require sensor nodes to match with one another, to match their sensing areas, and constitute a (K) anonymous cloaked regions. The resource algorithm aims to minimize both communication cost and computational cost, while the quality aware algorithm helps to minimize the cloaked regions, in order to increase the accurateness of aggregate locations that are reported.

Each sensor node in the resource-aware algorithm finds a standard no. of objects and then finds a cloaked area. Alternatively, the quality-aware algorithm takes place from a mapped region (A) computed by the resource aware algorithm. Now (A) will be

iteratively filtered based on additional communication between the sensor nodes until it reaches a minimal possible area. In both these algorithms, the sensor nodes report the cloaked area and the no. of monitored objects in that region. This will eventually be the aggregate location to the server. Whereas our system only identifies the aggregate location information of the monitored persons. It can still report "the no. of objects in a certain region." A spatial histogram analyses the aggregate locations to evaluate the distribution of monitored objects in the system.

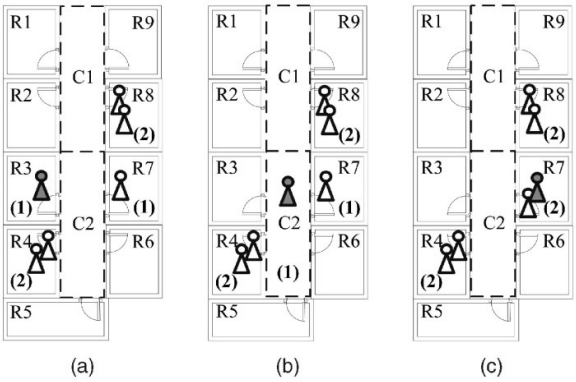



Fig.. A location monitoring system using counting sensors

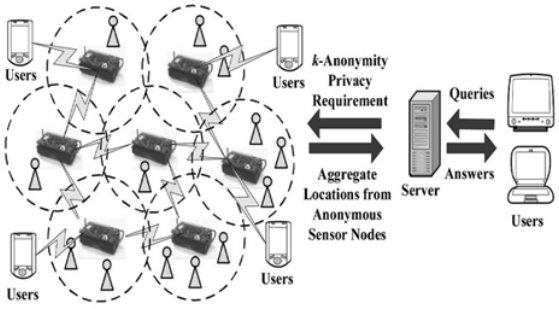



Fig. System Overview

## 2. SYSTEM MODEL

The above illustration in Fig.2 shows the design of the proposed system. Here, we have three main entities: sensor nodes, server, and system users. First let us define the problem to evaluate the objective and privacy settings of the model.

A set of sensor nodes S1, S2, S3, S4….,Sn with detecting areas A1, A2, A3, A4….An respectively and a set of moving objects O1, O2, O3, O4…,Om with a req. anonymity level k, we deduce that :

1. Aggregate location for each sensor node S is in the form of Ri= ( Areai,N i), where Area is a rectangular region that consists the sensing region of a set of sensor nodes S and N is the no. of items present in that sensing areas of the sensor nodes in S, such

that $N\ I \geq k$ , $N\ i=| \cup sj \in Si\ Oj| \geq k$ ,$Oj = \{ ol| ol \in aj \}$,$1 \leq i \leq n$ , and $1 \leq l \leq m$ ;

2. A spatial histogram method helps to answer the aggregate question (Q) that questions about the total no. of objects in a certain region (A). Area is reported by the sensor nodes based on the aggregate locations.

Sensor nodes determine the no. of objects in their sensing area by mapping its sensing area into a cloaked region (A) that includes at least (K) objects. This finds the no. of objects located in the mapped region as the aggregate location information to the server. Whatever may be the network type, our system only requires a communication channel from each sensor node to the server. Each sensor node is responsive of its location and detecting area.

The server assembles the aggregate locations information reported by the sensor nodes using a spatial histogram and evaluates the distribution of the monitored objects. Thus, answers the queries based on the estimated object distribution range. Moreover, the value of (K) is changed by administrator at any time by issuing / sending a message with a new value of (K) to all the sensor nodes. Authorized administrators and users can issue a range of queries to the system. These queries can be sent either to the server or to the sensor nodes, as shown in Fig. 2. The server answers the issued queries with the help of a spatial histogram.

This system also delivers anonymous communication between the server and sensor nodes by using the existing anonymous communication techniques. Moreover, only authorized administrators can access and change the (K) anonymity level and the scope of the spatial histogram. In certain cases, the administrators set the (K) anonymity level to a small value for more accurate aggregate locations from the sensor nodes. It may be even set to zero and disable the algorithm to get the original evaluations from the sensor nodes. This will be useful in facilitating the best services from the monitored system. Server or/and system users outside the trusted zone are considered untrusted.

Coming to the privacy threat in existing location monitoring systems, an identity-sensor reports the precise location information of each monitored object to their respective servers. So the rival can easily know the precise location information of each object. Similarly, if the number of objects in a monitored area is too small, the rival can suppose the identity of the monitored objects by mapping the monitored area

For instance, a woman is in her office room at time instance T1 as referred in Fig. 1. Here, this system only permits one sensor node to report (K) anonymous aggregate location to the server. With this, the rival cannot deduce an object's exact location. Larger the anonymity level (K), the more difficult it becomes for the rival to deduce the object's exact location.

The (K) anonymized aggregate locations information reported from the sensor nodes, will provide a poor location monitoring service for a small area, and an excellent quality services for huge/larger areas which will be indicated on the spatial histogram at the server. This is a highly effective approach to preserve the privacy of an object.

# 3. LOCATION ANONYMIZATION ALGORITHM

The two in-network anonymization algorithms: resource aware and quality aware are periodically performed by sensors to report their (K) varying aggregate locations to the server.

### 3.1 The Resource Aware Algorithm

The Resource Aware Algorithm illustrates the concept with 7 sensor nodes assuming from A to G. The required anonymity level is taken as 5 which means, K ¼ 5.
To prove this, we need a sensing area for the sensor nodes, and a dividing line between the two sensor nodes to indicate that the two sensor nodes can communicate directly with each other. The algorithm is executed in three phases.

Resource aware location anonymization
Algorithm

1: function RESOURCE-AWARE (Int k, Sensor m ,List R)
2: Peer List
**// Phase 1: The broadcast Phase**
3: Send a msg by m's authentication m:ID, sensing region m:Area, and object count m:Count to m's neighbour peer
4: if Receive a msg from a peer x, i.e., (x: ID, x: Area, x: count) then
5: Add msg to Peer List
6: If m gets required no. of objects then
7: Send an alert message to m's neighbours
8: if some m's neighbour has not found required number of objects then
9: Transfer the message to m's neighbours
10: end if
**// Phase 2: The cloaked area phase**
11: S fmg
12: Calculate score for every peer in Peer List

13: Select peer with highest score from Peer List to S till the total no. of objects in S is at least repeatedly.

14: Area a min. surrounding area of the Senor in S

15: N , the total no. of objects in S

**// Phase 3: The validation phase**

16: if No relation with Area and R2R then

17: Forward Area; NÞ to remaining peers within the region & server

18: elseif m's sensing region is mapped by some R2R then

19: Randomly select R02R where R0:Area mapping m's range

20: Forward R0 to peers under R0: Region & server

21: else

22: Return region with mapped N to peers in the region & the server

23: end if

### 3.2 The Quality Aware Algorithm

The quality aware algorithm considers the cloaked area calculated by the Resource Aware algorithm as the initial solution. Now, this quality-aware algorithm refines it until the cloaked area has reached the minimum. This still fulfils the required (K) anonymity privacy setting based on the added communication between other ends. The

quality aware algorithm by using the input initial solution terminates the existing minimal cloaked region containing the set of sensor nodes that creates the minimal sensing area. This algorithm again has three phases.

Quality Aware Algorithm

1: function QUALITY-AWARE (Int k, Sensor m, Setinit-solution, List L)
2: current minimum cloaked area init-solution
**// Phase 1: The search space phase**
3: Assume a search area S based on init-solution
4: Calculate the info of peer located in the area
**// Phase 2: The minimum cloaked region phase**
5: Add each node located in the area(S) to C½ as an object
6: Add m to each object in C½ as the initial object
7: for j ¼ 1; i 4; j ++ compute
8: for each item set X ¼ ga1 ; --- ; aiþ1 in C½ compute
9: if Area S MBR XÞÞ < Area (current minimum cloakedarea) then
10: if Nð MBR ðXÞ Þ k then
11:current minimum cloaked region fXi
12: Delete X from C½
13: end if
14: else
15: Prune X out of C½
16: end if
17: end for
18: if j< 4 then
19: for each object pair X ¼ gx1; . . . ; xiþ g,Y ¼gy1;...;yiþ1in C½ compute
20: if x1 ¼ y1; . . .. ;xi ¼ y & xiþ1 ¼ yiþ1 then
21: Add an object gx1; . . . ; xiþ1; yiþ1gto C½ þ 1
22: end if
23: Close for
24: Area a min. bounding rectangle of current minimum cloaked area
25: N , total no. of items in current minimum cloaked area
**// Phase 3: The validation phase**
26: Lines 16 to 23 in Alg. 1

### 3.2.1 Proof of Correctness

Here, the objective is to show the perfection of the quality aware location anonymization algorithm.

**Theorem 1:**

Assumed a resource aware cloaked area (A) of a sensor node (s), a search space (S) is computed by the quality aware algorithm comprises the least cloaked region.

**Proof:**

Suppose X is the minimal cloaked area equal to or less than the Area, in size. It is

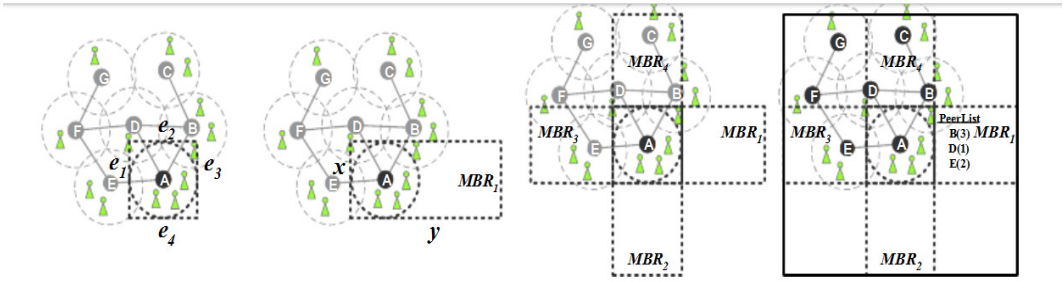
understood that X should totally cover the sensing range of s. If X is not completely covered by S, X must contain at least one stretched MBR, MBRi, where1i=4. i.e., region of X is greater than the region of extended MBR, Area. This denies the assumption that X is the minimum cloaked area. Hence X is with in S.

**Theorem 2:**

A minimal mapped rectangle can be termed by maximum four sensor nodes.

**Proof**

Assume, in an MBR, each edge of MBR touch the sensing location of one or another sensor node. In a hypothetical case, there is a separate sensor node touching some edge of the MBR, however no other edges. The MBR can be explained by four sensor nodes that touch different edge of the MBR. If more sensor nodes touch edge e but no other edges, it simply picks up one of those sensor nodes, because any of the sensor nodes give the same e. Hence, an MBR can be named by a minimum four sensor nodes.




(a) The MBR of $A$'s sensing area (b) The extended $MBR_1$ of the edge $e_1$ (c) The extended $MBR_i$ $(1 \leq i \leq 4)$ (d) The search space $\mathcal{S}$

## 4. SPATIAL HISTOGRAM

Spatial histogram is imbedded inside the server to evaluate the dissemination of the monitored objects created on aggregate location reported from different sensor nodes. The spatial histogram is indicated by a two-dimensional arrangement that models a grid shape and N columns; hence, the system space is partitioned into NR*N disjoint same-sized grid cells. Each cell U ( I , j ), a float value is maintained, and that acts as an estimator T [ i, j ] (1<=i<=N, 1 <=j <=NR) of the no. of items within the region. Imagine that the system has the capability to identify the total no. of moving items M in the system. The value of M is the initial value given to the spatial histogram. In practice, M can be computed for both moving/dynamic environments (indoor and outdoor). For the interior region, the sensor nodes can be deleted at each entry and exit to count the no. of users entering or exiting the system. For the outdoor setting, the sensor nodes have already been used to count the no. of people in a particular area. Using spatial histogram we provide approx. location monitoring services. The correctness of the spatial histogram, highlights the utility of our privacy-preserving Quality aware location monitoring system.

## 5. PERFORMANCE METRICS

System is evaluated in terms of 5 performance factors.

1. Catch model error

This model measures the flexibility of the system to the model with the help of relative error approach between the assessed no. of items N in the sensing region of a sensor node and the N= 0,we take N as error. Then the error is measured as ib.

2. Communication cost

The measure of communication cost of our location anonymization algorithms is the avg no. of bytes sent by the sensor nodes during the reporting period. This measure also displays the network traffic and the power
consumption by the sensor nodes.

3. Cloaked region size

It computes the quality of the average locations reported by the sensor nodes. The lesser the area, the better the correctness of the aggregate location.

4. Computational cost

This metric calculates the computational cost of our location aware algorithms in terms of the avg. number of the MBR computations that are required to find a resource/quality aware mapped/cloaked area. We then cross-check our algorithms with a basic approach which calculates the MBR for all combinations of peers in the formed search space to find the minimum cloaked region. The basic approach doesn't use any improvement techniques proposed for the quality aware algorithm.

5. Query error

This metric process the usage of the system, in terms of the relative error between the query reply, which is the estimated no. of items in the query area based on a spatial histogram, and actual reply M, respectively.

## 6. EXPERIMENTAL RESULTS & ANALYSIS

Here , analysing the experimental results w. r. to the privacy protection & quality aware of location monitoring services in the system.

### 6.1 Anonymization Strength

Above Fig. is the resilience of the system to the attacker model w.r. to the anonymity level and the total no. of objects. In the fig., the performance of the algorithms is as shown. Fig. a shows that, the rigid the anonymity level, the more the assailant model error will be in worse. When the anonymity level gets restricted, our algorithms generate larger cloaked regions, which minimize the accuracy of the aggregate locations reported to the server. Fig-b shows the attacker model. The error reduces, as the no. of objects gets more. This is because when there are more items, our algorithms generate smaller cloaked regions, which increase the accuracy of the average locations reported to the server. So that it is difficult to set a hard quantifiable threshold measure for the attacker model error. However, it is clear that the adversary cannot conclude the number of objects in the sensor node's sensing area with any fidelity.

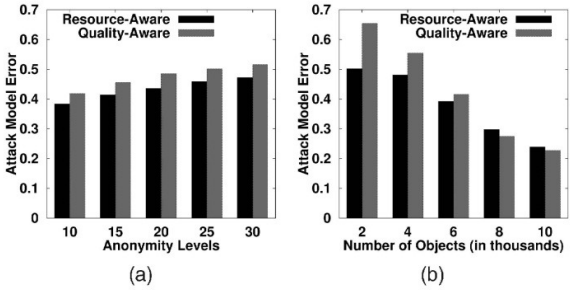



Figure: (a) Anonymity levels. (b) Number of objects

## 6.2 Effect of Query Area Size

Quality aware and Privacy guard of our location monitoring system w. r. to increase in the query region size ratio range from 0.0001 to 0.256, where query region size ratio is the ratio of the cloaked region to the system area and the query region size ratio 0.0001 that corresponds to the size of a sensor node's sensing area. Thus the results are evident that the system provides low quality location monitoring services for the range query with a small query region, and better quality services for higher query regions. This is an important feature to protect personal location privacy, because providing the accurate number of objects in a small area could reveal individual location information; therefore, an adversary cannot use our system output to track the monitored objects with any fidelity.

## 6.3 Effect of Increase in Number of Objects

The performance of our system w. r. to increase in the no. of items from 3,000 to 10,000.When the no. of objects increases, the communication cost of the resource-aware algorithm is effected slightly, whereas the quality aware algorithm significantly lowers the communication cost. Broadcast step of the resource aware alg. effectively allows each sensor node to search for adequate number of objects to map its sensing area. When there are more items, the sensor node finds smaller cloaked regions that satisfy the k anonymity privacy condition.

## 6.4 Effect of Privacy Conditions

With respect to change in the required anonymity level k from Ten to Forty. When the k-anonymity privacy level of requirement gets stricter, the sensor nodes have to enlist more no. of peers for help to blur/map their sensing areas; hence, the communication cost of our algorithms grows. To meet these, the stricter anonymity levels which our algorithms generate larger cloaked areas. For the quality aware alg., since there are more peers in the required search space when the input (resource aware) cloaked region gets larger, the computational cost of computing the minimal cloaked region by the quality aware alg. and the basic approach gets so bad. However, the quality aware algorithm minimizes the computational cost of the original approach by at least four times of magnitude. Larger cloaked regions give more wrong average location information to the system, so the estimation error grows as the required k anonymity increases. The quality aware algorithm provides effective quality location monitoring services than the other algorithm, when the required anonymity level gets more restricted.

### 6.5 Effect of Movements

Results show that increase in the object movement speed only slightly affects the communication cost and the cloaked region size. Since the resource-aware cloaked regions are less affected by the mobility speed, the object mobility speed has a very low effect on the required search area computed by the quality aware algorithm. Thus, the computational cost of the other algorithm is also less affected by the object moving speed. Although the query reply error gets worse when the objects mobility is faster, the query accuracy of the quality aware algorithm is regularly better than the resource aware algorithm.

## 7. CONCLUSION

In this paper, we propose a Quality aware location monitoring system for wireless sensor networks. Sketch of two in-network location anonymization approaches, namely, resource and quality-aware algorithms that preserves personal location details, while assigning the system to provide location monitoring services. Both algorithm approaches rely on the well-defined k anonymity privacy theory which requires a person is uniquely identified among k persons. In our system, sensor nodes process our location anonymization techniques to provide k anonymous aggregate locations, in which each average location is a cloaked region A with the no. of monitored objects, N, located in A, where N k, for the system. The resource aware algorithm helps to minimize communication cost and computational cost, while the quality aware algorithm helps to minimize the size of cloaked regions in order to generate more accurate specific locations. To guide for location monitoring services based on the summation of location information, we used a spatial histogram technique that analyses the aggregate locations reported from the sensor nodes to calculate the distribution of the monitored objects. The calculated distribution is used to provide location monitoring services by responding range queries. We evaluate our system based on simulated experiments. The results show that our system exhibits high-quality location monitoring services (the accuracy of the resource-aware algorithm is 75 %(approx..) and the accuracy of the quality-aware algorithm is 90 percent(approx..)), while preserving the monitored object's location privacy.

### ACKNOWLEDGEMENTS

This work was done by the M.Tech. student of St.Ann's College of Engg. & Technology, Chirala affiliated JNTU, Kakinada for the 2nd Year Academic Project. I express my sincere thanks to my guide and Head, Department of Computer Science and Engineering, Dr. P. Harini for her valuable suggestions during our course period. I would like to thank our principal, Dr. C. SubbaRao, Management of St. Ann's College of Engineering & Technology for providing me a pleasant environment and excellent laboratory facilities.

## REFERENCES

[1] B Bamba, L Liu, P. Pesti, And T. Wang, " Supporting Anonymous Location Queries in Mobile Environments with Privacy grid," Proc. International Conference World Wide Web , 2008.

[2] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, "TheCricket Location-Support System," Proc. ACM MobiCom, 2000.

[3] K. Bohrer, S. Levy, X. Li, and E. Schonberg, "Individualised Privacy Policy Based Access Ctrl," Pro. 6th Int'lConf.Electronic Commerce Research (ICECR), 2003.

[4] L. Sweeney, "Achieving k-Anonymity Privacy Protection UsingGeneralization and Suppression," Int'l J.Uncertainty, Fuzziness & Knowledge-Based Systems, vol. 10, no. 5, pp., 571-588, 2002.

[5] Traf-Sys Inc., "Pupil Counting Systems, " http://www.trasys.com/products/people-counters/thermal-sensor.aspx, 2009.

[6] M. Grutser, G. Schele, A. Jain, R. Han, and D. Grunwald,"Privacy-Aware Location Sensor Networks," Pro. Ninth Conf. Hot Topics in Operating Systems (HotOS), 2003.

[7] S. Guo, T. He, M.F. Mokbel, J.A. Stankovic, and T.F. Abdelzaher,"On Accurate and Efficient Statistical Counting in Sensor-Based Surveillance Systems," Proc. Fifth IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS), 2008.

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

[9] Title 47 US Code Section 222 (h) (2), http://frwebgate.acces.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid= Cite:+47USC222, 2009.

[10] D. Culler & M.S. Deborah Estrin, "Overview of Sensor Networks," Computer, vol. 37, no. VIII, pp. 41-49, Aug. 2004.

[11] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar,"SPINS: Security Protocols for Sensor Networks," Proc. ACM MobiCom, 2001.

[12] J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks," Proc.ACMMobiHoc, 2003.

[13] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "EnhancingSource-Location Privacy in Sensor Network Routing," Proc. 25thIEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2005.

[14] G. Kaupins and R. Minch, "Legal and Ethcal Implication of Employee Location Monitoring," Pro.38th Ann. Hawai Int'l Conf. System Sciences (HICSS), 2005.

[15] B. Son, S. Shin, J. Kim, and Y. Her, "Implementation of the Real-Time People Counting System Using Wireless Sensor N/w,"Int'l J. Multimedia and Ubiquitous Eng.,vol.2,no.2,pp.63-80,2007.

[16] E. Snekkenes, "Concept for Personal Location Privacy Policies,"Pro. 3rd ACM Conf. Electronic Commerce (EC), 2001.

[17] Onesystem Technology, "Counting People inBuilding," http://www.onesystemtech.com.sg/index.php?option=com_ content&task=view&id=10, 2008.

[18] H. Kido, Y. Yanagisaw, And T. Satoh, "An AnonymousComunication Technique Using Dummies for Location-Based Services," Pro. Int'l Conf. Pervasive Services (ICPS), 2005.

[19] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, " The Anatomy of a Context Aware Application," Proc. ACM Mobi Com, 1999.

Dr. P.Harini, Ph.D.
SACET, Chirala
Andhra Pradesh, INDIA
*(hpogadadanda@yahoo.co.in)*

**Dr.P.Harini** received B.E. degree in Electronics and Communications Engg. from University of Madras, Chennai, in1993, received M.Tech. degree in Remote Sensing from JNTU, Hyderabad, in 1997, received M.Tech. degree in Computer Science and Engineering from JNTU, Hyderabad,in 2003 and received Ph.D. in Computer Science and Engineering from JNTU, Anantapur, in 2011. She has 16 Years of

Experience in which 1 year of Industrial, 1 year of Research & over 14 years of rich Teaching Experience in reputed Engineering Colleges & She is currently working as Professor & HOD in Computer Science & Engineering department in St.Ann's College of Engineering & Technology, Chirala. She Published 21 Research papers in various International Journals & Conferences. Guided many UG & PG students for projects & Life time Member of ISTE & CSI. Conducted successfully many Workshops, Seminars, conferences, FDPs and many National Level Technical Symposiums

M.B.Raghavendra,
II-M.Tech.
Sacet, Chirala
mbraghav@gmail.com

**M.B.Raghavendra** Received B.Tceh. degree in Computer Science & Engineering from Chirala Engg. College, Chirala, in 2007 and pursuing M.Tech. in Computer Science & Engineering in St.Ann's College of Engg. & Technology.