RESEARCH ARTICLE OPEN ACCESS

A Novel Solitude Conserving Location Monitoring Approach for Wireless Sensor Networks

Pravallika. K* Suvarna. K** Chakrapani. T***
*,**,***(Department of Electronics and Communication Engineering, JNTU-Anantapur , SJCET, Kurnool)

ABSTRACT

Observing individual locations with a capable untrusted server impose secrecy threats to the monitored individuals. In this paper we propose “A Novel Solitude Conserving Location Monitoring approach for Wireless Sensor networks”. We design two approaches to study nondescript locations in-network approaches, namely quality-aware and resource-aware approaches, that aims to enable the system to give high end quality location monitoring services for end users, while conserving personal location privacy. Both approaches are worked based on k-anonymity solitude (i.e.,an object is indistinguishable among k objects), to enable highly trusted sensor nodes to provide the collective location data of monitored objects for our system. Each collective location is in a form of a observed area X along with the number of monitored objects reside in X. The resource-aware approach objective to optimize the computational and communication value, while quality-aware approach aims to increase the reliability of the collective location data by reducing their observing areas. We use spatial histogram methodology to estimates the distribution of observing objects based on the gathered collective location data. We evaluated these two approaches through simulated experiments. The simulation results shows that these approaches gives high quality location observing services for end users and assure the location secrecy of the monitored objects.

***Keywords* -** Anonymity, location, solitude spatial histogram, wireless sensor network

I. INTRODUCTION

Wireless sensor network is an emerging technology for many new application domains for agriculture, wild animal monitoring, habitat monitoring, battle field. Most of the cases of these applications rely on the information of individual locations, eg: soldier in the battle field and location systems in coal mines. Location dependent approaches are realized by using either identity or counting sensors. Bat Teleporting[3] is an event base method which gives a pinpoint absolute location of the individual object time to time. Cricket [4] follows the same as above and address the goals privacy, decentralized administration, low cost, network heterogeneity and portion of a room granularity. In above two approaches each and every individual sensor sends receives signal along with the global unique identifier. On the other side, counting sensors and thermal sensors are deployed in the physical area which reports the total number of objects situated in their sensing environment to a central application server. [21] Application counts the number of persons on the mountain area within a certain range of distance i.e, around 1.5m. Casper [1] location anonymizer utilizes a complete pyramid shape to index mobile users and blur their exact locations into cloaked areas. On the other hand, the versatile location anonymizer uses an incomplete pyramid shape for the location anonymization task.[2] sensor nodes evaluate our location anonymization approachs to provide k- anonymous aggregate points.[7] strengthen user secrecy protection compared to solutions at the database level because it *prevents collection* of privacy-sensitive data. [11] discussed about the ethical and legal implication of employee location observation. However, privacy violation may be considered when the employer’s monitoring has been physically violation and has no legitimate business purpose.[10] explains design and implementation of SNEP security protocol for wireless sensor networks which provides data confidentiality , two way authentication with low overhead. Identity sensor immediately poses a major security where as counting sensors provides collective location information and also provides privacy beaches.

This paper illustrates a privacy-preserving location monitoring system for wireless sensor networks to provide location monitoring services. Our approach relies on the well established k-anonymity privacy theme, which requires each object to be indistinguishable among k objects. In our system, each sensor node blurs its sensing area into a cloaked area, in which at least k objects are residing. Each sensor node reports only aggregate location information, which is in a form of a cloaked area, X, along with the number of objects, N, located in X, where N ≥ k, to the server. It is important to note that the value of k achieves a trade-off between the strictness of secrecy protection and the quality of monitoring services. X smaller k indicates less privacy protection, because a smaller cloaked area will be reported from the sensor node. However, a larger k results in a bigger cloaked area, which will decrease the quality of monitoring services, but it gives better privacy protection. Although our approach only knows the aggregate location information about the monitored objects, it can still provide monitoring features through answering aggregate queries, for example, How many number of objects in a certain area?. To support these monitoring services, we propose a spatial histogram that analyzes the gathered collective locations to estimate the distribution of the monitored objects in the system. The estimated distribution is used to address aggregate queries. For small cloaked area our proposed approach avoid privacy leakage by providing low quality service on the other hand provides high quality service for larger cloaked areas.

II. RELATED WORK

Straightforward techniques are followed for conserving users location privacy that comprise stipulated privacy policies. They moderate the usage of an access control model for privacy protection based on notion of purpose [8], [5] and anonymizing the stored data before any declaration by providing a formal presentation of combining generalization and suppression to achieve k-anonymity. Generalization involves replacing a valve with a less specific but semantically consistent valve. Suppression involves not releasing a valve at all [6].However these techniques fail to prevent internal information theft or unintended declaration. Presently, the personal location information is anonymized before any server collects it by using the location anonymization techniques to protect personal location privacy in location based services. These techniques are based on one of the three concepts.(1) *False Locations:* In this scheme, a client system produces several false position data's called dummies, which the system sends along with the true data of the object to the service provider [12]. (2) *Spatial Cloaking:* This technique permits users to express their privacy necessities in terms of location hiding by using Privacy Grid scheme(contains three dynamic grid dependent spatial cloaking approaches) where it blurs the users location into a cloaked spatial area [22], P2P spatial cloaking approach permits the mobile user to entertain anonymous location-dependent services without the aid of any centralized third parties [13], Clique Cloak Permutation engine technique [23] can effectively anonymize data sent by the mobile clients in conformity with location k-anonymity while full filling the privacy and QoS needs of the users. [15] PRIVE users who issue location-dependent queries arrange themselves into a hierarchical overlay network and anonymize queries in a fully decentralized manner. PRIVE supports our hilbASR anonymization approach, which assures anonymity under any user distribution. [16] MobiHide, a scalable P2P system for anonymous LBS queries. MobiHide registers objects into a hierarchical Chord network, according to the 1-D Hilbert grouping of their coordinates, and builds K-ASRs by indiscriminately choosing Hilbert sequences of K users. [9] The quadtree-based algorithm reached accuracy to assure k-anonymous location information through demotion in location resolution and empirically analyzed using a traffic distribution model derived from traffic counts and cartographic material, [17] conceal the user coordinates, by substituting them with a spatial region (either a circle or a rectangle). This region covers the query initiator and at least $K-1$ other users and examined their tradeoffs. [14] Casper; a new scheme in which mobile users can entertain location-based services without the need to reveal their private location information. Mobile users enrole with Casper by a user-specified privacy profile. Casper has two main modules, the location anonymizer(address accuracy, quality, capability, and flexibility) and the privacy-aware query approach (tune data base servers and their functionalities to be privacy-aware by associating with cloaked spatial areas rather than exact point information). [24] PIR(Private Information Retrieval) theory to guarantee secrecy in location-based queries, optimizations that acquire reasonable communication and CPU cost and addresses correlation attacks effectually.[18] *CPDA* and *SMART* pay attention to additive data aggregation functions in terms of privacy-conservation capability, communication and computational overhead, aggregation accuracy.[19] pDCS derive from Euclidean Steiner Tree and Bloom Filter to reduce the query message overhead , maximize the query privacy and afford different levels of location secrecy and provide a tradeoff between privacy and query efficiency.[20] SPYC prescribe query mechanisms that are communication efficient while significantly improving client query secrecy levels.

III. SYSTEM MODEL AND IMPLEMENTATION

Fig 1 delineate the architecture of the present study mainly three entities, server, sensor nodes and system users. The server gathers the aggregated locations using spatial histogram distribution of the monitored objects, and evaluated through answering range queries. Each sensor node is answerable for deciding the number of objects in its sensing place. System users are the administrator and the end users. Administrators had wide authentication and authorization rules maintained by LDAP servers.

Secrecy model : sensor nodes are established in a trusted zone, where they act as defined in our approach and communicate with each other through an authenticated network channel to avoid internal network attacks, for example, eavesdropping, traffic analysis, and malicious nodes [7].

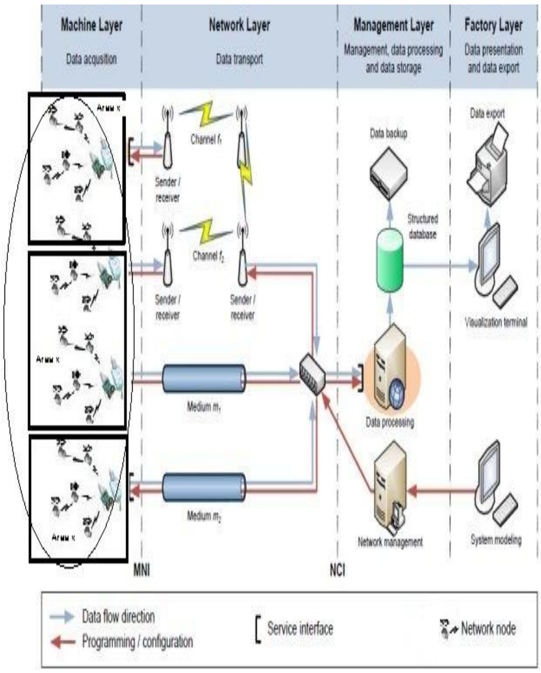


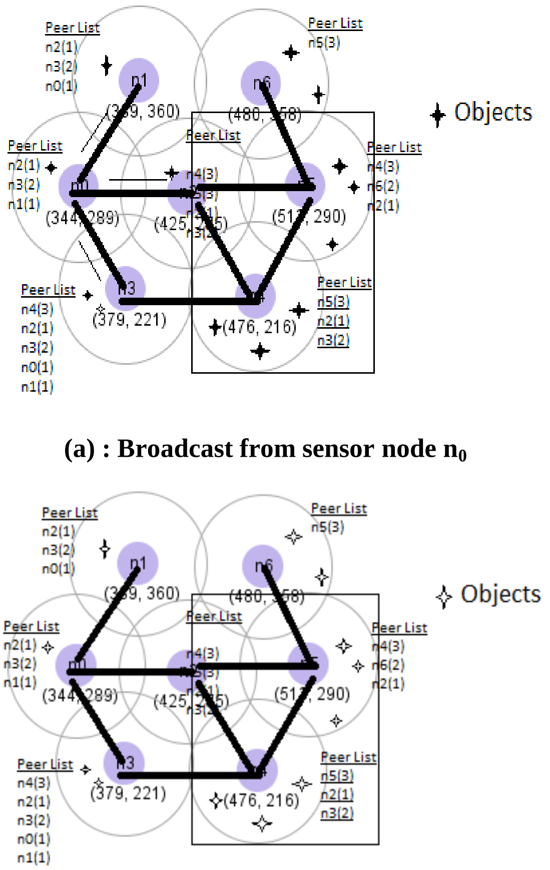
Fig 1.System Architecture

Problem definition: Given a set of sensor nodes n_1 , n_2 , ... , n_3 with sensing areas x_1, x_2 , ..., ,x_n respectively a set of moving objects o_1, o_2 ,....., ,o_m and a required anonymity level k. First find an aggregate location for each sensor node sn_i in a form of $R_i = (Area_i \, ; \, N_i)$,where $Area_i$ is a rectangular area containing the sensing area of a set of sensor nodes sn_i and N_i is the number of objects residing in the sensing areas of the sensor nodes in sn_i.Second answer the aggregate query by using spatial histogram.

To solve the above considerations we proposed two novel approaches first one resource- and quality-aware location anonymization algorithms that executed based on the periodical time slots and updates the level of annonimity to the central server.

3.1 Resource-Aware Approach

Fig2 illustrate the example resource-aware algorithm contains seven sensor nodes, n_0 to n_6 , and the required anonymity level k = 5. Each circular form shows the sensing area for individual sensor node, and dark line represents the direct connectivity between two sensor nodes . The Resource-aware approach is organized into three steps, namely Broadcast step,Cloaked area step,Validation step. The detailed design of these steps as follows.



(a) : Broadcast from sensor node n_0

(b) : Cloaked area of sensor node n_4

Fig2: The Resource-aware location anonymization algorithm (k = 5)

Step 1 : Broadcast Step : This step mainly focuses on adequate no.of objects to form a colaked area. To optimze the communication cost , this step relies on a heuristic that each sensor node only forwards its messages to its neighbours if it has found the required no.of objects in it .Each sensor node should contain a minimum (k=5) no.of objects in its sensing area.. Initially each sensor node *n* creates an empty *Peerlist pr*, later on *n* sends its message which includes its identity *n.id*,sensing area *n. Area*, no.of objects in that sensing area *n.count*, to its neighbours only when it has found an adequate no.of objects in it.In the same way when *n* receives a message from a peer *pr* i.e., (*pr.id*,*pr.area*,*pr.count*),then *n* stores the message in its *Peerlist.*

Algorithm 1
Resource aware location anonymization

```
1.  function resource aware (integer k, sensor n,
    list A)
2.  peerlist←{Ø}
    //Step 1: The Broadcast step
```

```
send a message with n`s identity n.ID,sensing area n.area,and
    object count n.count to n`s neighbour peers
if Receive a message from a peer pr,i.e (pr.ID,pr.Area,pr.count) then
Add the message to peerlist
if n has found an adequate no.of objects then
Send a notification message to n`s neighbours
end if
if some n`s neighbour has not found an adequate no.of objects then
Forward the message to n`s neighbours
end if
end if
//Step 2: The cloaked area step
T←{n}
Compute a score for each peer in peerlist
Repeateadly select the peer with highest score from peerlist to
    T untill the total no.of objects in T is atleast k
Area←a minimum bounding rectangle of the sensor nodes in T
N←total no.of objects in T
//Step 3: The validation step
If no contaiment relationship with Area and A □ A then
send (Area,N) to the peers within Area and the server
else if n`s sensing area is contained by some A □ A then
Randomly select a À □ A such that À. Area contains n`s sensing area
Send
    À to the peers within À. Area and the server
else
Send Area with a cloaked N to the peers within Area and the server
end if
```

Fig 2a illustrates the broadcast step. When process begins, each sensor node sends a msg to its neighbours.when the sensor nodes n_0 to n_6 has found the specified no.of objects then they sends a notification msg to its neighbours.Here the node n_0 has not received any notification msg from its neighbour n_1,then n_0 forwards its information about nodes n_1, n_2 and n_3 to n_1.Thus ,now node n_1 has found an adequate no.of objects and sends a notification msg to its neighbour n_0. At last all the nodes have found the required no.of objects, they proceed to next step.

Step 2: The Cloaked Area Step : The idea behind this step is that each nodes converts its sensing area into a cloaked area with a principle that it should contains minimum *k* objects in it. To reduce computational cost, this step uses greedy approach to find a cloaked area based on the information stored in *Peerlist.* For each node n initiates a set *T = {n}*,and caluclates a score for each peer in its *Peerlist.* Score is defined as a ratio of object count of the *peer* to the euclidean distance between the *peer* and *m.* In this manner with the help of score a set of *peers* are choosen from the *Peerlis*t to *T* to form a cloaked area as small as possible. Then frequently select the *peer* with the highest score from the *Peerlist* to *T* until *T* contains at least k objects. At last , *n* determines the cloaked area (Area) that is a *minimum bounding rectangle* (MBR) that includes the sensing area of the sensor nodes in *T*, and the total number of objects in *T* (N).

Fig 2b shows the cloaked area step. The *PeerList* of sensor node n_4 maintains the details of three peers, n_5 , n_2 , and n_3. From the fig object count of sensor nodes n_5 , n_2 , and n_3 is 3, 1, and 2, respectively. Let the distance from sensor node n_4 to sensor nodes , n_5 , n_2 , and n_3 be 19, 20, and 17, respectively. The score of n_5 , n_2 , and n_3 is 3/19 = 0.15, 1/20 = 0.05, and 2/17 = 0.11, respectively. Thus n_5 is selected, for obtaining the highest score. The sum of the object counts of n_4 and n_5 is six which is higher than the required anonymity level k = 5, so we represent the MBR of the sensing area of the sensor nodes in *T*, i.e., n_4 and n_5, as the resource-aware cloaked area of n_4, which is represented by a rectangle shape.

Step 3 : The Validation Step: Its mainly used to prevent reporting aggregate locations with a containment relationship to the server. Let A_i and A_j be two aggregate locations reported from sensor nodes i and j, respectively. If A_i*'s* observed area is included in A_j *'s* observed area, A_i*.Area* ⊂ *Aj.Area* or *Aj.Area* ⊂ *Ai.Area*, then its said that A_i and A_j have a containment relationship, then such nodes are not permitted to report their aggregate locations to server, because combining such aggregate locations may cause privacy leakage. For example, if A_i*.Area subset* A_j*.Area* and A_i*. Area≠* A_j *.Area*, then the number of objects residing in the non-overlapping area, A_j*. Area –* A_i *.Area*, is A_j*. N –* A_i*.N.* If A_j*. N –* A_i*.N < k*, then the number of objects residing in the non-overlapping zone is less than k it means that it violates the k-anonymity principle . As this step confirms that no aggregate location with the containment relationship should be reported to the server, the adversary cannot obtain any deterministic information from the aggregate locations.

3.2 Quality-aware Approach

The primary solution to the quality-aware approach is the cloaked area obtained from the resource aware approach, this solution is processed until the cloaked area achieve the minimal possible area. The quality aware approach initializes a variable *current minimal cloaked area* by the input primary solution. When the approach concludes, the *current minimal cloaked area* comprises the set of sensor nodes that forms the minimal cloaked area. The quality-aware approach is organized into three steps, namely Search space step, Minimal cloaked area step, Validation step. The detailed design of these steps is as follows.

Step 1: The search space step: As there are huge no.of sensor nodes in a conventional sensor network, its very expensive for a sensor node *n* to collect the information of all the sensor nodes to determine its minimal cloaked area. To minimize the computational and communication cost *search space*, *T*, is computed based on the cloaked area obtained by the resource-aware approach, such that the sensor nodes outside *T* are not included in the minimal cloaked area

Step 2: The minimal cloaked area step: It aims to determine the minimal cloaked area for each sensor node *n* by considering a set of peers located in the search space, *T*, as an input. Searching all the feasible combinations of the peers is costly. Thus we propose optimization techniques to minimize the computational cost. The objective behind an optimization technique is that its not necessary to analyse all the combinations of the peers in *T*, rather, we only need to review the combinations of atmost four peers. This technique determines the MBR by taking into consideration atmost four sensor nodes because among them two sensor nodes define the width of the MBR (parallel to the x-axis) while the remaining two other sensor nodes define the height of the MBR (parallel to the y-axis). Thus this technique mainly optimizes the computational cost by minimizing the number of MBR computations among the peers in *T*.

Step 3: The Validation step*:* This step is exactly the same as in the resource-aware approach.

The pseudo code related to Quality aware approach is as represented in the below algorithm 2.This algorithm explains about all the three steps followed in quality aware approach.

Algorithm 2
Quality aware location anonymization

```
public void Qualityaware(int k<
  sensor>m,set<int>in,list<integer>R)
cmca=in
  // Step 1: The search space step
string S[ ]=determine(in)
li.add(S[i])
list<integer> li=m list <integer>
for(integer  i:S)
   count=0
for(integer k: li)
   li.add(S[i])
  //Step 2: The minimal c loaked area step
if(count<4)
   k[i]=k[i].add(m)
   if(area MBR(k_i)<Area(cmca)) then
      if(MBR(k).count( )≥k) then
      cmca=k
      li.remove(k)
else
   li.remove(k)
      end if
count++
else
break
  //Step 3:The validation step
Same as  validation step in  Algorithm 1
```

3.3 Spatial histogram

Spatial histogram that is fixed inside the server used to evaluate the distribution of the observed objects based on the aggregate locations informed from the sensor nodes. Our spatial histogram is described by a two-dimensional array in the form of a grid structure *G* of C_R rows and C_{col} columns ; hence, the system space is divided into $C_R \, X \, C_{col}$ disjoint equal sized grid cells. In each grid cell *G*(i, j), we maintain a fractional value that acts as an estimator H[i, j] (1 ≤ i ≤ $C_{col}, 1 \leq j \leq C_R$) of the number of objects within its area. We assume that the system has the ability to know the total number of moving objects *O* in the system. The value of *O* initialize the spatial histogram later. In practice, *O* can be calculated for dynamic environments(both indoor and outdoor). Spatial histogram mainly used to obtain approximate location monitoring services. The reliability of the spatial histogram that indicates the usage of our privacy preserving objects monitoring system will be evaluated .

Algorithm 3 summarizes our spatial histogram technique. Initially, we let the objects be uniformly distributed in the system, so the estimated number of objects within each grid cell is $H[i,j] = O/(C_R \, X \, C_{col})$. The initial valve of the histogram is a set of aggregate locations *A* transmitted from the sensor nodes. Each aggregate location A in *A* contains a cloaked area, A.Area, and the number of observe red objects within A.Area, A.N. Initially the aggregate locations in *A* are clubbed into the some partition $P = \{A_1, A_2, \ldots\ldots, A_p\}$ if their cloaked areas are not intersecting with each other, which means that for every pair of aggregate locations A_i and A_j in *P*, $A_i.Area \cap A_j.Area = \emptyset$.

Algorithm 3
Spatial histogram maintenance

```
public void histogram(set<integer<A)
for each sink location A □ A do
 if there is a partition  p={A_1, A_2,..... A_P}
such that A.Area ∩  A_k.Area = Ø for
every  A_k ϵ p  then
    p.add(A)
else
    creat partition(A)
    end if
end for
for(integer  i : partition)
        $H[i,j] = \left(\frac{ls_k .N}{cell\ count}\right)$
for(integer loc : partition)
        $A_k.\hat{N} = sum(G(i,j), powH[i,j])$
end for
$p.Area = sum\ of(A_1.area : A_p.area)$
   $H[i,j] = H[i,j] + \left(\frac{sum(ls_k)}{out\ cell\ count}\right)$
end for
```

Then, for each partition *P*, we upgrade its entire set of aggregate locations to the spatial histogram at the same time. For each aggregate location A in *P*, we report the estimation error, which is the difference between the sum of the estimators within A.*Area*, $A.\hat{N}$,and A.*N*, and then A.*N* is evenly distributed among the estimators within A.*Area*; hence, each estimator within A.*Area* is set to A.*N* divided by the total number of grid cells within A.*Area* . After operating all the aggregate locations in *P*, we sum up the estimation error of each aggregate location in *P*, $\sum_{k=1}^{|P|} A_k.\hat{N} - A_k.N$, that is evenly distributed among the estimators outside *P.Area*, where *P.Area* is the area covered by some aggregate location in *P*, $P.Area = \bigcup_{A_k \epsilon P} A_k .Area$. Normally, for initialize the spatial histogram later. In practice, *O* can be calculated for dynamic environments(both indoor and outdoor). Spatial histogram mainly used to obtain approximate location monitoring services. The reliability of
each partition *P* that contains |*P*| aggregate locations $A_k\ (1 \leq k \leq |P|)$,, every estimator in the histogram is upgraded as follows:

$$H[i,j] = \begin{cases} \dfrac{A_k.N}{\text{cell count within } A_k.N} & \text{for } G(i,j)\ \epsilon\ A_k.\text{Area} \\[2ex] H[i,j] + \dfrac{\sum_{k=1}^{|p|} A_k.\hat{N} - A_k.N}{\text{outer cell count P.Area}} & \text{for } G(i,j) \not\epsilon\ \text{P.Area} \end{cases}$$

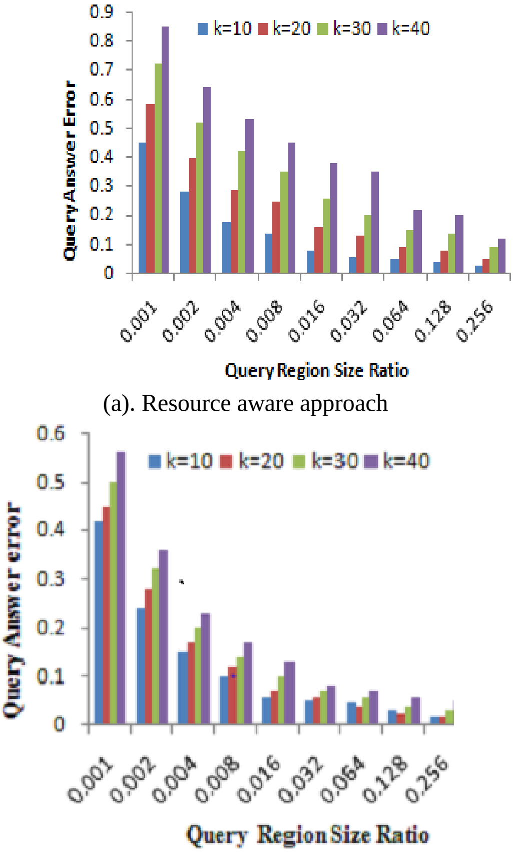
IV. SIMULATION SETTINGS

In all experiments, we simulate 50 ×50 sensor nodes that are evenly distributed in a 800 × 800 system space. Each sensor node is responsible for monitoring a 25 × 25 space. We generate a set of moving objects that freely roam around the system space. Unless mentioned otherwise, the experiments consider 6,000 moving objects that move at a random speed within a range of [0,5] space unit(s) per time unit, and the required anonymity level is k = 25. The spatial histogram contains $C_R\ X\ C_{col}$ = 200 × 200 grid cells, and we issue 1,000 range queries whose query region size is specified by a ratio of the query region area to the system area, that is, a query region size ratio. The default query region size ratio is uniformly selected within a range of [0.001 , 0.034].

V. SIMULATION RESULTS AND ANALYSIS

5.1. Effect of Query Region Size

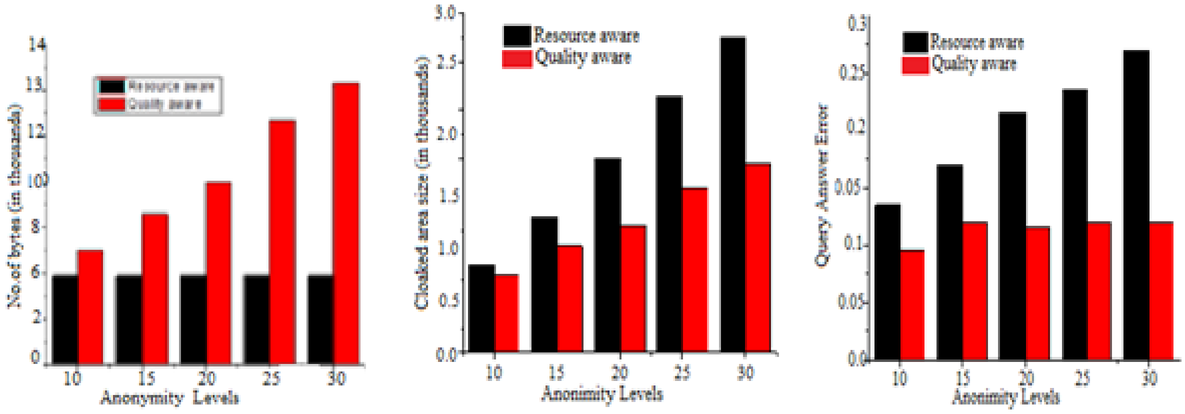
Fig 3 describes the secrecy and quality of the proposed location observing system with respect to increasing the query region size ratio from 0.001 to 0.256.where the query region size ratio(ratio of the query region area) to the system area and the query region size ratio 0.001 regard to the size of a sensor node's sensing area. therefore an unfavorable cannot use our system output to track the monitored objects with any fidelity. The definition of a small query region is relative to the required anonymity level k.



(a). Resource aware approach

(b). Quality aware approach

Fig. 3 : Query region size



(a) Communication cost (b) Cloaked area size (c) Estimation error

Fig 4 : Anonymity levels

For example, we want to provide low quality services, such that the query error is at least 0.2, for small query regions. For the resource-aware algorithm, Fig 3a shows that when k = 10, and the query region size is not larger than 0.002 (it is about two sensor nodes' sensing area) is said to be small. However, when k = 30, and the query regionsize is not larger than 0.016 (it is about 16 sensor nodes' sensing area) is said to be small. Fig 3b(quality aware algorithm) describes that when k = 10, and query region size is not larger than 0.002 is said to be small, while when k = 30, and query region size is not larger than 0.004 is only considered as small . The results also show that the quality-aware algorithm always performs better than the resource-aware algorithm.

5.2. Effect of Privacy Requirements

In terms of privacy Fig 4a (Communication cost), Fig 4b (cloaked area size) and Fig4c (Estimation error) illustrates the performance of proposed system with anonymity level k varies from 10 to 30. When the k-anonymity privacy requirement gets stricter, the sensor nodes have to enlist more nodes for help to blur their sensing areas, therefore the communication cost increases, generate larger cloaked areas of our proposed algorithms. For the quality-aware algorithm, since there are more nodes in the required search space when the input (resource aware) cloaked area gets bigger, the computational cost of computing the minimal cloaked area by the quality aware algorithm and the basic approach gets poor(Fig 4d).However, the quality-aware algorithm optimizes the computing cost of the basic approach by at least four orders of magnitude. Larger cloaked areas give more unreliable aggregate location information to the central system, so the estimation error increases with respect to k-anonymity.

In terms of Privacy quality aware provides superier than resource aware when the required anonymity level gets stricter.

VI. CONCLUSION

In this current proposed work we evaluated two anonymization approaches namely, *resource-* and *quality-aware* algorithms, that preserve individual location privacy, while enabling the system to provide reliable object monitoring services. Both approaches depend on the well established k-anonymity privacy concept that requires a person is indistinguishable among k persons. In our proposed system, sensor nodes execute our location anonymization approaches to provide accurate 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. To optimize the communication cost we proposed resource aware approach. While the quality-aware algorithm objective is to reduce the size of cloaked areas in order to generate more reliable number of aggregate locations. By using spatial *histogram* approach we analyzed aggregate locations reported from the sensor nodes to estimate the distribution of the observing objects for providing better object monitoring services with the help of range queries. We evaluated the current system through simulated experiments. The results describes the reliability of resource aware is 75% and for quality aware obtain 90% while preserving the monitored object's location privacy.
In future scope of implementation some of the other network properties will be investigate with different anonymity levels.

REFERENCES

[1]. One systems Technologies, Counting people in buildings.http://www.onesystemstech.com.sg/index.php?option=com content&task=view%&id=10.

[2]. Traf-Sys Inc., .People counting systems. http://www.trafsys.com/products/people counters/thermal-sensor.aspx..

[3]. A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, .*The anatomy of a context-aware application*,. in Proc. of MobiCom, 1999.

[4]. N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, .*The cricket location-support system*,. in Proc. of MobiCom, 2000.

[5]. E. Snekkenes, .*Concepts for personal location privacy policies*,. in Proc. of ACM EC, 2001.

[6]. L. Sweeney, .*Achieving k-anonymity privacy protection using generalization and suppression*,. *IJUFKS, vol. 10, no. 5,* pp. 571. 588, 2002.

[7]. M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, .*Privacy-aware location sensor networks*,. in Proc. of HotOS, 2003.

[8]. K. Bohrer, S. Levy, X. Liu, and E. Schonberg, *Individualized privacy policy based access control,. in Proc. of ICEC,* 2003.

[9]. M. Gruteser and D. Grunwald, *Anonymous usage of locationbased services through spatial and temporal cloaking*,. in Proc. Of MobiSys, 2003.

[10]. D. Culler and M. S. Deborah Estrin, .*Overview of sensor networks, . IEEE Computer, vol. 37, no. 8,* pp. 41.49, 2004.

[11]. G. Kaupins and R. Minch, .*Legal and ethical implications of employee location monitoring*,. in Proc. of HICSS, 2005.

[12]. H. Kido, Y. Yanagisawa, and T. Satoh, *An anonymous communication technique using dummies for location-based services*,. In Proc. of ICPS, 2005.

[13]. 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.

[14]. 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.

[15]. G.Ghinita,P.Kalnis,and S.Skiadopoulos, PRIVE: *Anonymous location-based queries in distributed mobile systems*,. in Proc. Of WWW, 2007.

[16]. G. Ghinita1, P. Kalnis, and S. Skiadopoulos, .MobiHide: A mobile peer-to-peer system for anonymous location-based queries,. In Proc. of SSTD, 2007.

[17]. 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.

[18]. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, .PDA: *Privacy-preserving data aggregation in wireless sensor networks*,. in Proc. of Infocom, 2007.

[19]. M. Shao, S. Zhu, W. Zhang, and G. Cao, .pDCS: *Security and privacy support for data-centric sensor networks*,. in Proc. Of Infocom, 2007.

[20]. B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, .*Query privacy in wireless sensor networks*,. in Proc. of SECON, 2007.

[21]. 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.

[22]. B. Bamba, L. Liu, P. Pesti, and T. Wang, .*Supporting anonymous location queries in mobile environments with privacygrid*,. In Proc. of WWW, 2008.

[23]. 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.

[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.