High Quality Location Monitoring System with Location Privacy

John J P[1], Mamatha C M[2]
[1]Research Scholar, Dept. of CSE, MSRIT, Bangalore, Karnataka, India..
[2]Research Scholar, Dept. of CSE, NCET, Bangalore, Karnataka, India.

Abstract:- **While a wireless sensor network is deployed to monitor certain events and pinpoint their locations, the location information is intended only for legitimate users. However, an eavesdropper can monitor the traffic and deduce the approximate location of monitored objects in certain situations. Anonymizing wireless sensor networks allow users to access services privately by hiding the client's IP address from the server. As a result, administrators block all anonymous access to misbehaving. Location privacy is an important security issue. Loss of location privacy can enable subsequent exposure of identity information. Monitoring personal locations with a potentially untrusted server poses privacy threats to the monitored individuals; a high quality location monitoring system with location privacy for wireless sensor networks is adopted. Two in-network location anonymization algorithms are considered, namely, resource and quality-aware algorithms that aim to enable the system to provide high-quality location monitoring services for system users, while preserving personal location privacy. Both algorithms rely on the well established k-anonymity privacy concept, that is, a person is indistinguishable among k persons, to enable trusted sensor nodes to provide the aggregate location information of monitored persons. Each aggregate location is in a form of a monitored area A along with the number of monitored persons residing in A, where A contains at least k persons. The resource-aware algorithm aims to minimize communication and computational cost, while the quality - aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas. To utilize the aggregate location information and to provide location monitoring services, a spatial histogram approach is used that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then, the estimated distribution is used to provide location monitoring services through answering range queries.**

I. INTRODUCTION

A wireless sensor network(WSN) consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. With the spreading application of Wireless Sensor Networks (WSNs) in various sensitive areas such as health- care, military, habitat monitoring, *etc*, the need to ensure security and privacy is becoming imperatively important. For example, in battlefield application scenario, "the location of a soldier should not be exposed if he initiates broadcast query" [1]. In the meantime, query must be transferred to the destination in and encrypted manner via only trusted en-route nodes. Similarly, in habitat monitoring application scenarios, such as Great Duck Island [2] or Save-the-panda application [3] where large numbers of sensor nodes are deployed to observe the vast habitat of ducks and pandas, an adversary can try to capture the panda or duck by back-tracing the routing path until it reaches the source sensor nodes. Therefore, in order to prevent the adversary from back-tracing, the route, location and data privacy mechanisms must be enforced. Many cases of these applications rely on the information of personal locations, for example, surveillance and location systems. These location-dependent systems are realized by using either identity sensor or counting sensors. For identity sensors, for example, Bat [1] and Cricket [2], each individual has to carry a signal sender/receiver unit with a globally unique identifier. With identity sensors, the system can pinpoint the exact location of each monitored person. On the other hand, counting sensors, for example, photoelectric sensors [3], [4], and thermal sensors [5], are deployed to report the number of persons located in their sensing areas to a server.

Unfortunately, monitoring personal locations with a potentially untrusted system poses privacy threats to the monitored individuals, because an adversary could abuse the location information gathered by the system to infer personal sensitive information [2], [6], [7], [8]. For the location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server; thus using identity sensors immediately poses a major privacy breach. To tackle such a privacy breach, the concept of *aggregate location information*, that is, a collection of location data relating to a group or category of persons from which individual identities have been removed [8], [9], has been suggested as an effective approach to preserve location privacy [6], [8], [9]. Although the counting sensors by nature provide aggregate location information, they would also pose privacy .

This paper proposes a privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services. Our system relies on the well established k-anonymity privacy concept, which requires each person is indistinguishable among k persons. In our system, each sensor node blurs its sensing area into a *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 the server. It is important to note that the value of k achieves a trade- off between the strictness of privacy protection and the quality of monitoring services. A smaller k indicates less privacy protection, because a smaller cloaked area will be reported from the sensor node; hence better monitoring services. However, a larger k results in a larger cloaked area, which will reduce the quality of monitoring services, but it provides better privacy protection.

To preserve personal location privacy, we propose two in-network aggregate location anonymization algorithms, namely, *resource*- and *quality-aware* algorithms. Both algorithms require the sensor nodes to collaborate with each other to blur their sensing areas into cloaked areas, such that each cloaked area contains at least k persons to constitute a k- anonymous cloaked area. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of the cloaked areas, in order to maximize the accuracy of the aggregate locations reported to the server. In the resource-aware algorithm, each sensor node _nds an adequate number of persons, and then it uses a greedy approach to find a cloaked area. On the other hand, the quality-aware algorithm starts from a cloaked area A, which is computed by the resource-aware algorithm. Then A will be iteratively refined based on extra communication among the sensor nodes until its area reaches the minimal possible size. For both algorithms, the sensor node reports its cloaked area with the number of monitored persons in the area as an aggregate location to the server.

Although our system only knows the aggregate location information about the monitored persons, it can still provide monitoring services through answering aggregate queries, for example, .What is the number of persons in a certain area?. To support these monitoring services, we propose a *spatial histogram* that analyzes the gathered aggregate locations to estimate the distribution of the monitored persons in the system. The estimated distribution is used to answer aggregate queries.

2. SYSTEM MODEL

Fig.1 depicts the architecture of our system, where there are three major entities, sensor nodes, server, and system users. We will define the problem addressed by our system, and then describe the detail of each entity and the privacy model of our system.

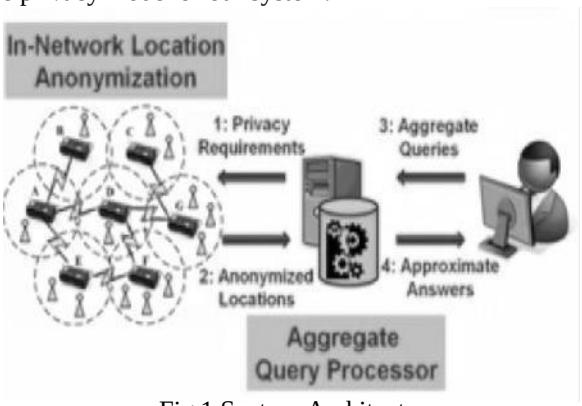

Fig 1 System Architecture

Sensor nodes. Each sensor node is res5yponsible for determining the number of objects in its sensing area, blurring its sensing area into a cloaked area A, which includes at least k objects, and reporting A with the number of objects located in A as aggregate location information to the server. We do not have any assumption about the network topology, as our system only requires a communication path from each sensor node to the server through a distributed tree [10]. Each sensor node is also aware of its location and sensing area.

Server. The server is responsible for collecting the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects, and answering range queries based on the estimated object distribution. Furthermore, the 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.

System users. Authenticated administrators and users can issue range queries to our system through either the server or the sensor nodes, as depicted in Figure
2. The server uses the spatial histogram to answer their queries.

Privacy model. In our system, the sensor nodes constitute a trusted zone, where they behave as de_ned in our algorithm and communicate with each other through a secure network channel to avoid internal network attacks, for example, eavesdropping, traf_c analysis, and malicious nodes [6], [11]. Since establishing such a secure network channel has been studied in the literature [6], [11], the discussion of how to get this network channel is beyond the scope of this paper. However, the solutions that have been used in previous works can be applied to our system.

Our system also provides anonymous communication between the sensor nodes and the server by employing existing anonymous communication techniques [12], [13]. Thus given an aggregate location R, the server only knows that the sender of R is one of the sensor nodes within R. Furthermore, only authenticated administrators can change the k-anonymity level and the spatial histogram size. In emergency cases, the administrators can set the k-anonymity level to a small value to get more accurate aggregate locations from the sensor nodes, or even set it to zero to disable our algorithm to get the original readings from the sensor nodes, in order to get the best services from the system. Since the server and the system user are outside the trusted zone, they are untrusted.

3. IMPLEMENTATION

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

3.1 Modules

A.WSN Location Monitoring Module

The location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server; thus using identity sensors immediately poses a major privacy breach. To tackle such a privacy breach, the concept of aggregate location information, that is, a collection of location data relating to a group or category of persons from which individual identities have been removed , has been suggested as an effective approach to preserve location privacy . Although the counting sensors by nature provide aggregate location information, they would also pose privacy breaches.

B. Aggregate locations Module

We design two in-network location anonymization algorithms, namely, 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 requires 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

C. Mapped Location monitoring Module

i. Sensor nodes.

Each sensor node is responsible for determining the number of objects in its sensing area, blurring its sensing area into a cloaked area A, which includes at least k objects, and reporting A with the number of objects located in A as aggregate location information to the server. We do not have any assumption about the network topology, as our system only requires a communication path from each sensor node to the server through a distributed tree . Each sensor node is also aware of its location and sensing area.

ii. Server.

The server is responsible for collecting the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects, and answering range queries based on the estimated object distribution. Furthermore, the 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.

iii. System users.

Authenticated administrators and users can issue range queries to our system through either the server or the sensor nodes, as depicted in Above System Architecture figure. The server uses the spatial histogram to answer their queries.

D. Minimum bounding rectangle (MBR)

We find the minimum bounding rectangle (MBR) of the sensing area of A. It is important to note that the sensing area can be in any polygon or irregular shape.

4. LOCATION ANONYMIZATION ALGORITHMS

In this section, we present our in-network resource-
And quality-aware location anonymization algorithms that is periodically executed by the sensor nodes to report their
k-anonymous aggregate locations to the server for every reporting period.

We provide 2 location anonymization algorithms namely,

1) **The Resource-Aware anonymization Algorithm**
2) **The Quality-Aware location anonymization Algorithm**

In addition to the above 2 algorithms we provide one more algorithm for calculating the aggregate location called, **Spatial histogram maintenance.**

4.1 The Resource-Aware Algorithm

This algorithm outlines the resource-aware location anonymization algorithm. Figure 3 gives an example to illustrate the resource-aware algorithm, where there are seven sensor nodes, A to G, and the required anonymity level is _ve, k = 5. The dotted circles represent the sensing area of the sensor nodes, and a line between two sensor nodes indicates that these two sensor nodes can communicate directly with each other. In general, the algorithm has three steps.
Step 1: The broadcast step. The objective of this step is to guarantee that 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.
Step 2: The cloaked area step. The basic idea of this step is that each sensor node blurs its sensing area into a cloaked area that includes at least k objects, in
Order to satisfy the k-anonymity privacy requirement. To minimize computational cost, this step uses a greedy approach to find a cloaked area based on the information stored in *PeerList*.
Step 3: The validation step. The objective of this step is to avoid reporting aggregate locations with a containment relationship to the server

Algorithm 1
1: **function** RESOURCEAWARE (Integer k, Sensor m, List R)
2: *PeerList* <-{}
// Step 1: The broadcast step
3: Send a message with m's identity m:ID, sensing area m:Area, and object
count m:Count to m's neighbor peers
4: **if** Receive a message from a peer p, i.e., (p:ID, p:Area, p:count) **then**
5: Add the message to *PeerList*
6: **if** m has found an 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 neighbors
11: **end if**
12: **end if**
// Step 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 is at least k
16: Area <- a minimum bounding rectangle of the senor 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 E *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 E *R* **then**
21: Randomly select an R' E R *such* that R0: 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**

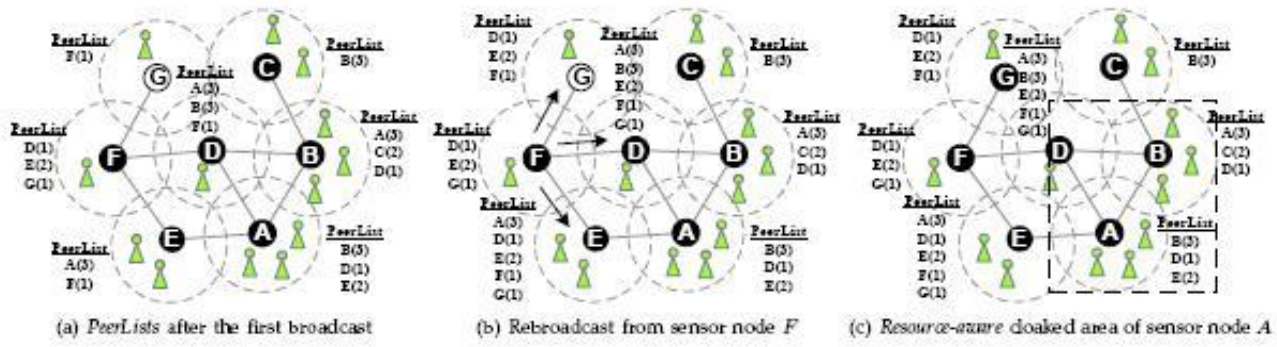

Fig. 2: The resource-aware location anonymization algorithm (k = 5).

4.2 The Quality-aware algorithm

This algorithm outlines the quality-aware algorithm that takes the cloaked area computed by the resource- aware algorithm as an initial *solution*, and then refines it until the cloaked area reaches the minimal possible area, which still satisfies the k-anonymity privacy requirement, based on extra communication between other peers. The quality-aware algorithm initializes a variable *current minimal cloaked area* by the input initial solution (Line 2 in Algorithm 2). When the algorithm terminates, the *current minimal cloaked area* contains the set of sensor nodes that constitutes the minimal cloaked area. In General, the algorithm has three steps.

Step 1: The search space step. Since a typical sensor network has a large number of sensor nodes, it is too costly for a sensor node m to gather the information of all the sensor nodes to compute its minimal cloaked area. To reduce communication and computational cost, m determines a *search space*, S, Based on the input initial solution, which is the cloaked area computed by the resource-aware algorithm, such that the sensor nodes outside S cannot be part of the minimal cloaked area (Line 3 in Algorithm 2). We will describe how to determine S based on the example given in Figure 4. Thus gathering the information of the peers residing in S is enough for m to compute the minimal cloaked area for m (Line 4).

Step 2: The minimal cloaked area step. This step takes a set of peers residing in the search space, S, as an input and computes the minimal cloaked area for the sensor node m.

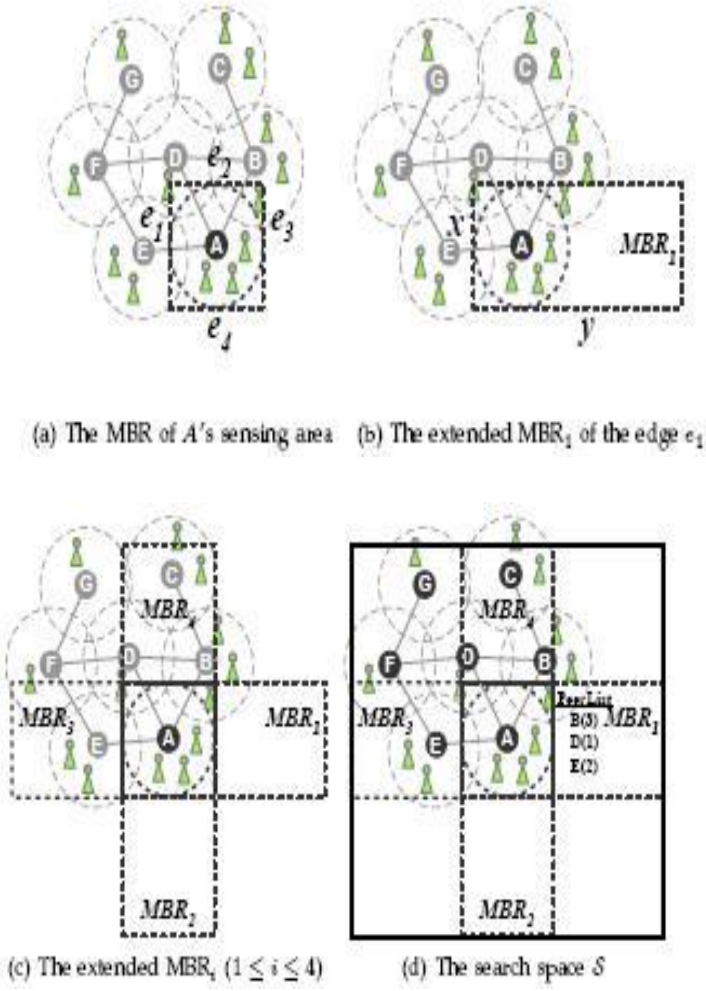

Fig. 3: The search space S of sensor node A.

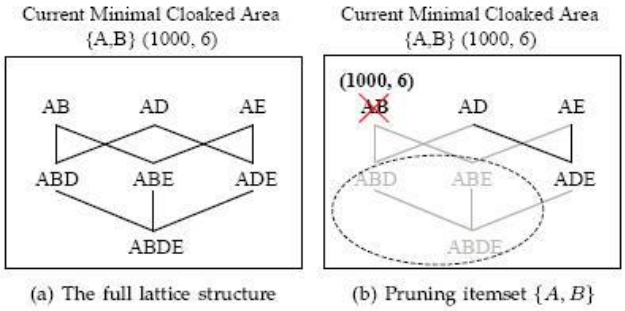

Fig 4: The quality aware cloaked area of sensor A.

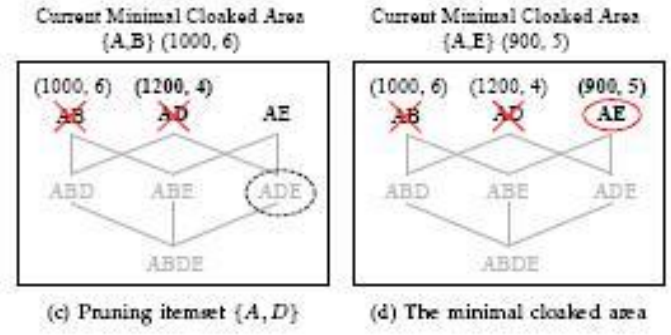

Fig 5: The quality aware cloaked area of sensor A & B.

Algorithm 2

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,….., ai+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,…,;xi+1}, Y ={y1,….,yi+1} in C[i]
do
20: **if** x1 = y1,…., xi = yi and xi+1 6 not equal to yi+1 **then**
21: Add an itemset {x1; : : : ; xi+1; yi+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

5. CONCLUSION

In this paper, we propose a privacy-preserving location monitoring system for wireless sensor networks.We design two in-network location anonymization algorithms,namely, *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 requires 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, while the quality-aware algorithm aims to minimize the size of cloaked areas in order to generate more accurate aggregate locations. To provide location monitoring services based on the aggregate location information, we propose a *spatial histogram* approach that analyzes the aggregate locations reported from the sensor nodes to estimate the distribution of the monitored objects. The estimated distribution is used to provide location monitoring services through answering range queries. We evaluate our system through simulated experiments. The results show that our system provides high quality location monitoring services (the accuracy of the resource-aware algorithm is about 75% and the accuracy of the quality aware algorithm is about 90%), while preserving the monitored object's location privacy.

6. 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] Onesystems Technologies, .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 of employee location monitoring,. in *Proc. of HICSS*, 2005.

[8] .Location Privacy Protection Act of 2001, http://www. techlawjournal.com/cong107/privacy/location/s1164i s.asp..

[9] .Title 47 United States Code Section 222 (h) (2), http://frwebgate.access.gpo.gov/cgi- bin/getdoc.cgi?dbname= browse usc&do%cid=Cite:+47USC222..

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

[11] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, .SPINS: Security protocols for sensor netowrks,. In *Proc. of MobiCom*, 2001.

[12] J. Kong and X. Hong, .ANODR: Anonymous on demand routing with untraceable routes for mobile adhoc networks,. in *Proc. Of MobiHoc*, 2003.

[13] P. Kamat, Y. Zhang,W. Trappe, and C. Ozturk, .Enhancing sourcelocation privacy in sensor network routing,. in *Proc. Of ICDCS*, 2005.

[14] S. Guo, T. He, M. F. Mokbel, J. A. Stankovic, and T. F. Abdelzaher, .On accurate and ef_cient statistical counting in sensor-based surveillance systems,. in *Proc. of MASS*, 2008.

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

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

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

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

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

[20] C. Bettini, S. Mascetti, X. S. Wang, and S. Jajodia, .Anonymity in location-based services: Towards a general framework,. in *Proc. of MDM*, 2007.

[21] 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.

[22] 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.

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

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