Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Conceptual Design of Location Monitoring System to preserve privacy in Wireless Sensor Networks.

Soumyasri S M [1], Dr.Rajkiran Ballal[2]
Dept. of Computer Science , SDM College, Ujire
Dept. of Electrical & Electronics Engineering, Marine College of Engineering, Mangalore.

Abstract: In potentially unreliable server through public network like internet, monitoring individual information, collected by sensors is threat to the individual privacy. Related to this we are proposing privacy preserving location monitoring system in wireless sensor networks. The objective of our system is to enable the system by providing high quality location monitoring services for system users, while preserving personal location privacy. Here design has been carried out with two advanced anonymization algorithm, namely *resource and quality aware algorithm.* Both algorithms rely on well known k-anonymity privacy concepts. In this concept, a person is indistinguishable among k persons, to enable trusted sensor nodes to provide the aggregate location information of monitored persons for our system. The main objective of resource aware algorithm is to reduce the communication and computational cost, while aim of quality aware algorithm is to maximize the accuracy of aggregate location information of monitored objects. The results shows that, our system guarantees the location privacy of the object and provide high quality location monitoring services.
Keywords: Wireless sensor networks, k-anonymization, aggregate location, cloaked area, location privacy.

I . INTRODUCTION

The advances in science and technology are deeply intervened. Peoples can use computers to visualize, through numerical simulation, physical phenomena, we cannot observe through empirical means. This trend has advanced with the prolonged exponential growth in the underlying semiconductor technology. A given computing capacity becomes exponentially smaller and cheaper with each passing year. Researchers can use the semiconductor manufacturing techniques that underlie this miniaturization to build radios and exceptionally small mechanical structures that sense fields and forces in the physical world. These inexpensive, low-power communication devices can be deployed throughout a physical space, providing dense sensing close to physical phenomena, processing and communicating this information, and coordinating actions with other nodes. Combining these capabilities with the system software technology that forms the Internet makes it possible to instrument the world with increasing fidelity.

The individual devices in a wireless sensor network (WSN) are inherently resource constrained: They have limited processing speed, storage capacity, and communication bandwidth. These devices have substantial processing capability in the aggregate, but not individually, so we must combine their many vantage points on the physical phenomena within the network itself. Wireless sensor networks could advance many scientific pursuits while providing a vehicle for enhancing various forms of productivity, including manufacturing, agriculture, construction, and transportation. In most settings, the network must operate for long periods of time and the nodes are wireless, so the available energy resources—whether batteries, energy harvesting, or both—limit their overall operation. Because they are so closely coupled to a changing physical world, the nodes forming the network will experience wide variations in connectivity and will be subject to potentially harsh environmental conditions. Their dense deployment generally means that there will be a high degree

of interaction between nodes, both positive and negative. Each of these factors further complicates the networking protocols.

Although computer-based instrumentation has existed for a long time, the density of instrumentation made possible by a shift to mass-produced intelligent sensors and the use of pervasive networking technology gives WSNs a new kind of scope that can be applied to a wide range of uses. These can be roughly differentiated into

- monitoring space,
- monitoring things, and
- monitoring the interactions of things with each other and the encompassing space.

The first category includes environmental and habitat monitoring, precision agriculture, indoor climate control, surveillance, treaty verification, and intelligent alarms. The second includes structural monitoring, eco physiology, condition-based equipment maintenance, medical diagnostics, and urban terrain mapping. The most dramatic applications involve monitoring complex interactions, including wildlife habitats, disaster management, emergency response, ubiquitous computing environments, asset tracking, healthcare, and manufacturing process flow. Dense instrumentation, real-time access, and in-network processing make a qualitative difference in our ability to perceive what is happening throughout large physical structures. In environmental monitoring and condition-based maintenance, the purpose of data collection, the parties responsible for using the data, and the scope of dissemination are clear. The situation becomes much less clear in more casual settings in which more general human activity occurs, such as the home, the workplace, a transportation terminal, or a shopping venue. In these cases, many potentially interested parties can have varying uses for the data.

Many of the applications like military and civilian purposes rely on the information of personal locations, for example surveillance and location systems. For all these applications preserving the privacy in location monitoring system is a primary need.

In this paper we propose latest technology to preserve the privacy in location monitoring system for wireless sensor networks. Here we come up with design of two efficient algorithm namely, *resource* and *quality aware algorithms*.

II. RELATED WORKS

The advance in wireless sensor technologies has resulted in many new applications for military and civilian purposes. In all these applications it is essential to maintain the privacy of the data from the location monitoring systems. These location sensor systems are implemented by either the identity sensors 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. By using identity sensors, it is possible to get the exact location of the monitored objects. On the other hand, to report the number of objects located in the sensing areas , counting sensors are widely used. For example, photoelectric sensors [3], [4] and thermal sensors [5]. Unfortunately, if the potentially untrusted system monitors the personal location, it may poses privacy threat to the monitored individual and gathered sensitive information about the object can be misused [6], [7], [8]. Since identity sensors in location monitoring system gives exact location of the object, it is an immediate threat to the privacy of the monitored object. In such cases to preserve the privacy, concept of *aggregate location information*, that is, instead of collecting individual object information, it gathers the location data relating to the group or certain kind of category of an monitored object [8], [9].

Several studies shows that every individual person concerned about their privacy[10]. According to Robinson[11], privacy is the top remaining issue for LBS. Within The World Wide Web Consortium (W3C), work on Privacy is being managed as part of W3C's Technology and Society domain. The W3C has several privacy-related activities, including P3P[12][13]. Advances in sensor networking and location tracking technology enable location-based applications but they also create

significant privacy risks. Privacy is typically addressed through privacy policies, which inform the user about a service provider's data handling practices and serve as the basis for the user's decision to release data. However, privacy policies require user interaction and offer little protection from malicious service providers. Privacy concerns in location-based application scenarios are typically addressed in a location broker residing in the middleware layer. To our knowledge, Spreitzer and Theimer [14] pioneered the development of such an architecture. In this work, each user owns a trusted user agent that acts as an intermediary. It collects location information from a variety of sensors and controls application access to this data. Wireless sensor networks have been widely used to monitor many types of environments such as battlefields [15], buildings [16] and habitats [17,18].

III. METHODOLOGY

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. Here only we requires a communication path from each sensor node to the server through distributed tree [19].

Servers: Servers responsible for collecting the aggregate information from the sensor nodes and to estimate the distribution of monitored objects, using spatial histogram, and answering the range queries

System Users: Authenticated administrators and other users can issue the range queries.

Privacy Model : Sensor nodes constitutes the trusted zone and communicates with each other through the secure networks to avoid the internal attacks.

3.1. LOCATION ANONYMIZATION ALGORITHM

Here we use following algorithms that is periodically executed by sensor nodes to report their k-anonymous aggregate locations.

3.1.1. Resource aware anonymization algorithm.

Algorithm 1 outlines the resource-aware location anonymization algorithm.
Figure 1 gives an example to illustrate the resource-aware algorithm, where there are seven sensor nodes, A to G, and the required anonymity level is five, 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.
Step 1: ***The broadcast step.*** *The purpose of this step is to guarantee that* each sensor node knows an adequate number of objects to compute a cloaked area. 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 to reduce the communication cost. . In this step, after each sensor node m initializes an empty list *PeerList* (Line 2 in Algorithm 1), m sends a message with its identity m:ID, sensing area m:Area, and the number of objects

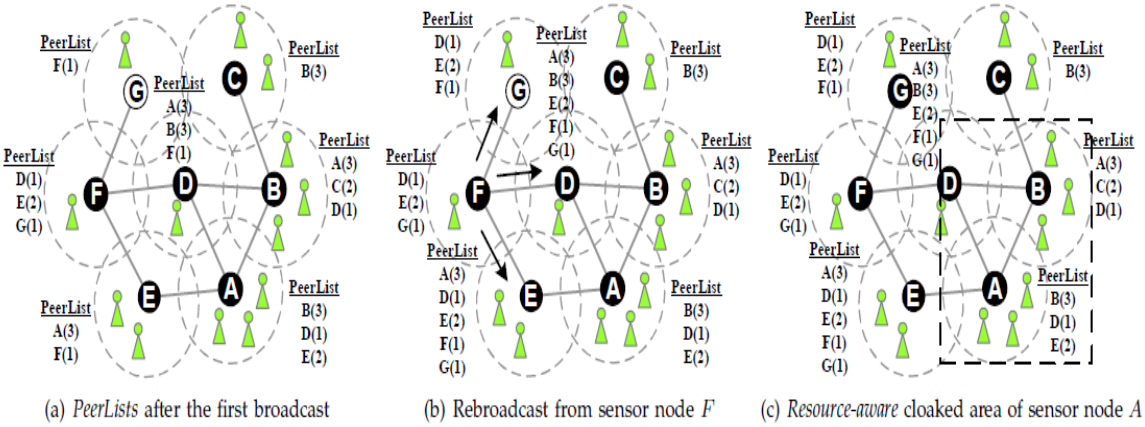


Figure. 1: Resource aware location [20]

located in its sensing area m:Count, to its neighbors (Line 3). When m receives a message from a peer p, i.e., (p:ID; p:Area; p:Count), m stores the message in its *PeerList* (Line 5). Whenever m finds an adequate number
of objects, m sends a *notification* message to its neighbors. (Line 7). If m has not received the notification message from all its neighbors, some neighbor has not found an adequate number of objects; therefore m forwards the received message to its neighbors. Figure 1a and 1b illustrates broadcast step. When a reporting period starts, each sensor node sends a message with its identity, sensing area, and the number of objects located in its sensing area to its neighbors. Once all the sensor nodes found the adequate number of objects in its sensing area, it proceeds for next step.

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. For each sensor node m, m initializes a set S = { m }, and then determines a score for each peer in its *PeerList* (Lines 13 to 14 in Algorithm 1). The score is defined as a ratio of the object count of the peer to the Euclidean distance between the peer and m. The idea behind the score is to select a set of peers from *PeerList* to S to form a cloaked area that includes at least k objects and has an area as small as possible. Then we repeatedly select the peer with the highest score from the *PeerList* to S until S contains at least k objects (Line 15). Finally, m determines the cloaked area (Area) that is a *minimum bounding rectangle* (MBR) that covers the sensing area of the sensor nodes in S, and the total number of objects in S (N). Figure 1c illustrates the cloaked area step.

Step 3: Validation Step. The objective of this step is to avoid reporting aggregate locations with a containment relationship to the server. We do not allow the sensor nodes to report their aggregate locations with the containment relationship to the server, because combining these aggregate locations may pose privacy leakage. For example, if Ri.Area ⊂ Rj.Area and Ri.Area ≠ Rj:Area, an adversary can infer that the number of objects residing in the non-overlapping area, Rj.Area – Ri.Area, is Rj.N – Ri.N. In case that Rj.N – Ri.N < k, the adversary knows that the number of objects in the non-overlapping is less than k, which violates the k-anonymity privacy requirement.

Algorithm 1

1.function *RESOURCE AWARE* (integer k, sensor m, list R.)
2.Initialise *PeerLis*t with null value.
Step 1:Announcement Step
3.Send a message with m's identity m.ID, m's area m.AREA, m's count m.COUNT. to the neighbor peers.
4. if Recieves the message from peer *p i.e (p.ID, p.AREA, p.COUNT), then*
5. Add the message to the *peerlist*.
6. *if* m has found enough number of objects, then
7. Send notification message to m's neighbor.
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. *endif.*
Step 2: The Cloaked Area Step
13. Initialize S with m value.
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.Assign the AREA with minimum bounding rectangle of the sensor node S.
17. Assign N with total number of objects in S.
Step 3: 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' € 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

3.1.2 The Quality Aware- Algorithm

Algorithm 2 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. 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).

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. Although the search space step already prunes the entire system space into S, exhaustively searching the minimal cloaked area among the peers residing in S, which needs to search all the possible combinations of these peers, could still be costly. Thus we propose two optimization techniques to reduce computational cost. The

basic idea of the first optimization technique is that we do not need to examine all the combinations of the peers in S; instead, we only need to consider the combinations of at most four peers. The second optimization technique has two properties, *lattice structure* and *monotonicity property*.

Algorithm 2: Quality Aware Location anonymization.

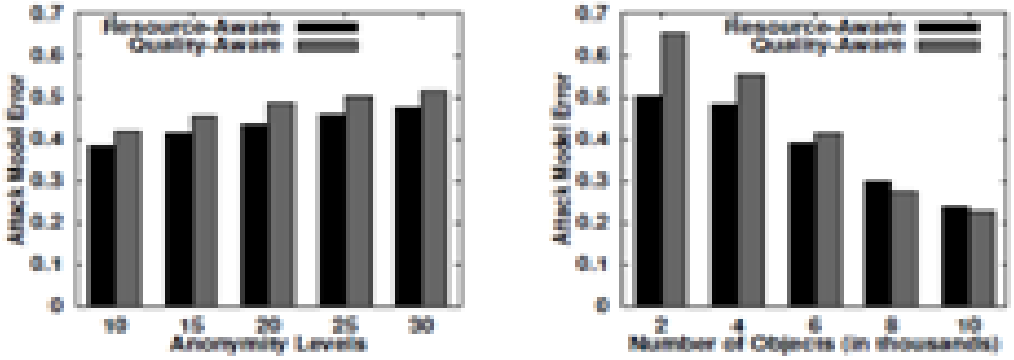
Step 3: The validation step. This step is exactly the same as in the resource-aware algorithm.

```
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+1g, Y =fy1…yi+1}  in C[i]
       do
20:      if x1 = y1… xi = yi  and x_{i+1} ≠ y_{i+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
```

IV. EXPERIMENTAL RESULTS

4.1 Anonymization strength

In this section, we show and analyze the experimental results with respect to the privacy protection and the quality of location monitoring services of our system.



(a) Anonymity Level (b) Number of Objects

Figure. 2 performances of the resource- and quality-aware algorithms

The Figure 2 depicts the performance of the resource and quality aware algorithm. Figure 2 a shows the stricter the anonymity level. When the anonymity level gets stricter, our algorithms generate larger cloaked areas, which reduce the accuracy of the aggregate locations reported to the server. Figure 2b shows that the attacker model error reduces, as the number of objects gets larger. This is because when there are more objects, our algorithms generate smaller cloaked areas, which increase the accuracy of the aggregate locations reported to the server. However, it is evident that the adversary cannot infer the number of objects in the sensor node's sensing area with any fidelity.

4.2 Effect of Query Region Size

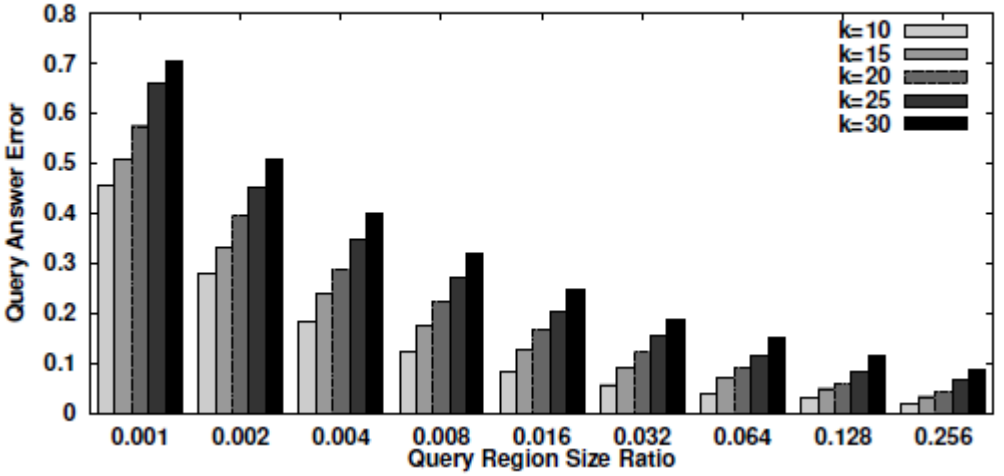
Figure 3 depicts the privacy protection and the quality of our location monitoring system with respect to increasing the query region size ratio from 0.001 to 0.256, where the query region size ratio is the ratio of the query region area to the system area and the query region size ratio 0.001 corresponds to the size of a sensor node's sensing area. The results give evidence that our system provides low quality location monitoring services for the range query with a small query region, and better quality services for larger 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.

Figure 3a shows that when k = 10, a query region is said to be small if its query region size is not larger than 0.002 (it is about two sensor nodes' sensing area). However, when k = 30, a query region is only considered as small if its query region size is not larger than 0.016 (it is about 16 sensor nodes' sensing area). For the quality aware algorithm, Figure 3b shows that when k = 10, a query region is said to be small if its query region size is not larger than 0.002, while when k = 30, a query region is only considered as small if its query region size is not larger than 0.004. The results also show that the quality-aware algorithm always performs better than the resource-aware algorithm.

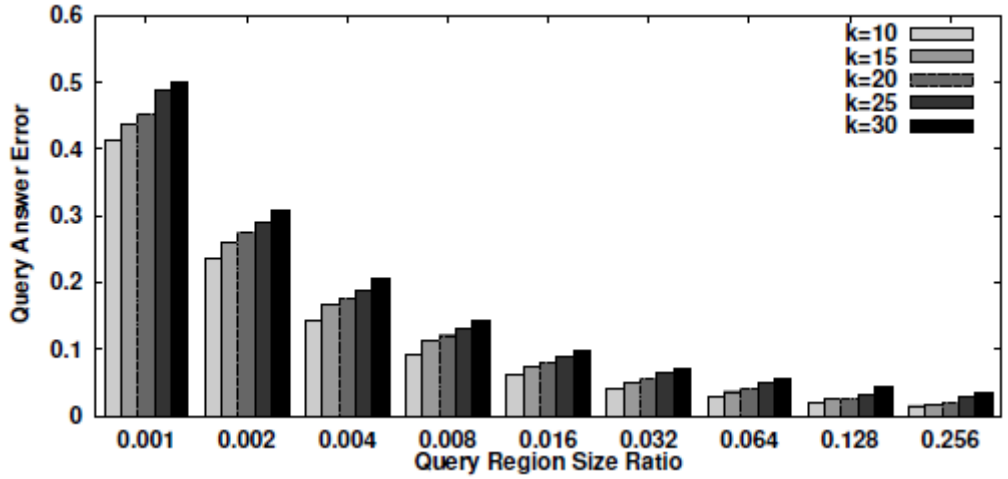
4.3 Effect of Privacy Requirements

Figure 4 depicts the performance of our system with respect to varying the required anonymity level k from 10 to 30. When the k-anonymity privacy requirement gets stricter, the sensor nodes have to enlist more peers for help to blur their sensing areas; therefore the communication cost of our algorithms increases (Figure 4a). To satisfy the stricter anonymity levels, our algorithms generate larger cloaked areas, as depicted in Figure 4b. For the quality-aware algorithm, since there are more peers in the required search space when the input (resource aware) cloaked area gets larger, the computational cost of computing the minimal cloaked area by the quality aware algorithm and the basic approach gets worse (Figure 4c). However, the quality-aware algorithm reduces the

computational cost of the basic approach by at least four orders of magnitude. Larger cloaked areas give more inaccurate aggregate location information to the system, so the estimation error increases as the required k-anonymity increases (Figure 4d).

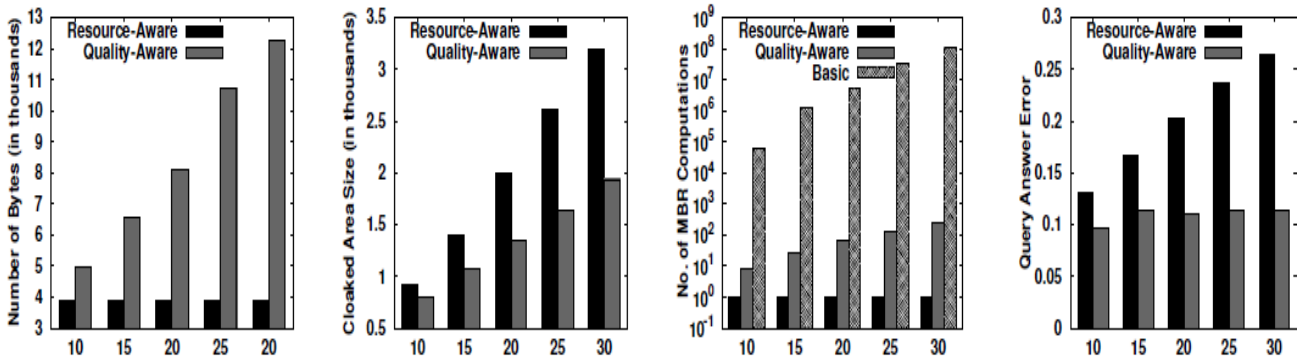


(a) Resource-Aware algorithm.[20]



(b) Quality aware algorithm [20]

Figure 3. Query Region Size



(a) Communication cost(b) Cloaked Area Size (c) Computational Cost(d) Estimation Error

Figure 4.Anonymity Levels [20]

V. CONCLUSION

In this paper, we propose location Monitoring System to preserve privacy in 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 $\geq$ 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. The results show that our system provides high quality location monitoring services (the accuracy of the resource-aware algorithm is about 70% and the accuracy of the quality aware algorithm is about 80%), while preserving the monitored object's location privacy.

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/s1164is.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]. Fox, S. The Internet Life Report. Trust and Privacy Online: Why Americans Want to Rewrite the Rules. The Pew Internet & American Life Project. August 20, 2000. http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_ Report.pdf.
[11 Robinson, T. Location is everything. Internet week online, tuesday September 12, 2000. http://www.internetwk.com/lead/lead091200.htm
[12] W3C. P3P and Privacy on the Web FAQ. http://www.w3.org/P3P/P3FAQ
[13] W3C. Platform for Privacy Preferences (P3P) Project. http://www.w3.org/P3P
[14] Mike Spreitzer and Marvin Theimer. Providing Location Information in a Ubiquitous Computing Environment. In *Proceedings of the Fourteenth ACM Symposium on Operating System Principles*, pages 270–283, 1993.
[15] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko, A. Vora, and M. Miyashita. A Wireless Sensor Network for Target Detection, Classification, and Tracking. *Computer Networks (Elsevier)*, 2004.
[16] Vipul Singhvi, Andreas Krause, Carlos Guestrin, Jr. James H. Garrett, and H. Scott Matthews. Intelligent light control using sensor networks. In *SenSys '05*, 2005.
[17] R. Szewczyk, A. Mainwaring, J. Anderson, and D. Culler. An Analysis of a Large Scale Habit Monitoring Application. In *SenSys'04*, 2004.
[18] Geoff Werner-Allen, Jeff Johnson, Mario Ruiz, Jonathan Lees, and Matt Welsh. Monitoring Volcanic Eruptions with a Wireless Sensor Network. In *EWSN '05*.
[19] D. Culler and M. S. Deborah Estrin, Overview of sensor networks, . *IEEE Computer*, vol. 37, no. 8, pp. 41.49, 2004.
[20] Chi-Yin Chow, Mohamed F. Mokbel, and Tian He are with the Department of Computer Science and Engineering, University of Minnesota, Minneapolis, MN 55455, USA, email: fcchow, mokbel, lianheg@cs. umn.