International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

# A Privacy-Preserving Location Monitoring System For Wireless Sensor Networks

**Harshitha G P[1], Dr Mahesh K Kaluti[2]**

*[1]M Tech, CSE, Dept. of Computer Science and Engineering, PESCE, Mandya,*
*[2]Assistant professor, CSE, Dept. of Computer Science and Engineering, PESCE, Mandya*

---

**Abstract—***The ultimate development in communication results in ever increasing application areas of the wireless sensor networks. Wireless sensor networks are widely used for location monitoring. Location Monitoring systems are used to detect human activities and provide monitoring services .It's need in the confidential area is still oscillating objective due to security threats. The privacy threats by the untrusted server affect the individual being monitored. Here, we design two innetwork location anonymization algorithms, the main aim to enable the system to provide high quality location monitoring services for system users, while preserving personal location privacy. The algorithms used rely on the well established k-anonymity privacy concept, 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.*

***Keywords— wireless sensor network, location monitoring, aggregate location, privacy preserving.***

## 1. Introduction:

Advances in sensor devices and wireless communication technologies have resulted in many new applications for military and civilian purposes, in which Location monitoring and surveillance are also part of these applications [5]. The location monitoring systems are implemented by using two kinds of sensors. They are counting sensor and identity sensor. The identity sensors are meant for pinpointing exact location of persons in given location while the count sensors are meant for reporting the number of persons present in the given location.

Monitoring personal locations required a server being used for location query processing. The server is essentially an Internet server and therefore it is untrusted. Such server may cause potential risk to the privacy of individuals being monitored. This is because hackers might be able to get sensitive personal information through compromised server. The identity sensors especially provide exact location of individuals being monitored which causes privacy breaches when hacked from server. The counting sensors also provide information related to count of people being monitored. It also breaches privacy when hacked by adversaries [10].

Aggregate location monitoring is one of the key applications. Aggregate location monitoring has a simple form of "What is the number of objects in a certain area". In general, aggregate location monitoring systems provide several valuable services that include: (1) Density queries, e.g., "determine the number of moving objects within a specified query region", (2) Safety control, e.g., "send an alert if the number of persons in a certain area exceeds a predefined threshold", and (3) Resource management, e.g., "turn off some building facilities if the number of people in a prespecified area is below a certain threshold". Real-life applications of location monitoring include employee tracking in workplaces, patient tracking in hospitals, and surveillance networks. Such location monitoring systems rely on deploying either identity or counting sensors. Identity sensors communicate with a small wireless transmitter attached to human bodies to determine human's exact locations and identities. On the other side, counting sensors are able to determine the number of objects or people within their sensing areas. Thus, the counting sensor is able to report only aggregate location information, i.e., its sensing area along with the number of detected objects within the sensing area, to a server.

Privacy is a critical issue when applying theoretical research in wireless sensor networks to scientific, civilian and military applications. e.g., environmental sensing, smart transportation and enemy intrusion detection [3]. Wireless sensor networks are vulnerable to privacy breaches because they possess the following characteristics

•**Wireless communication:** Wireless sensors need to communicate with each other through wireless communication. Wireless communication signals are easy to be tracked or eavesdropped by adversaries.

• **Open environments:** Wireless sensor Networks are usually deployed in open environments to provide sensing and monitoring services. Such open environments could cause privacy concerns because malicious people can easily approach the system area or even physically access the sensor.

• **Large-scale networks:** The number of sensor nodes in a WSN is often large, so that protecting every node from being compromised by adversaries is difficult. Thus, the privacy enhancing technology designed for the WSN should be able to deal with a situation that the network contains some compromise sensor nodes which can be controlled by adversaries.

• **Limited capacity:** In general, wireless sensors have scarce resources, e.g., limited computational power, constrained battery power, and scarce storage space.

Due to these limitations, it is very challenging to design secure privacy-preserving techniques for Wireless sensor networks.

The three main types of privacy for existing Wireless sensor network applications, namely, system privacy, data privacy, and context privacy. For example, in an event detection application, the location information of source sensor nodes is the sensitive information and can be inferred by adversaries through wireless communication signal analysis even without knowing the transmitted data content. Such event detection applications require system privacy protection. In a data collection application, its sensor node's readings are sensitive and should be protected during the course of transmission. Thus, data collection applications need data privacy protection. In a location monitoring application, the location information of monitored individuals is sensitive and should be protected. Location monitoring applications call for context privacy protection. From these three applications, we can see that different types of WSN applications have their own definition of sensitive information and they require different privacy protection techniques [1].

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, 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.

## 2. System model

Figure 1 depicts the system architecture of our aggregate location monitoring system that consists of three major components, wireless sensor network, aggregate query processor and resource-efficient sensor scheduler. We consider a set of sensor nodes s1,s2,...,sn and a set of moving objects o1,o2,...,om. The extents of two or more sensing areas may overlap. An aggregate location is defined as a reading from a sensor node si in a form of (Areai, Ni) where Areai is si's sensing area and Ni is the number of detected objects within Areai, Given a system area S. Area and a continuous stream of aggregate locations (Area, N) reported from a set of sensor nodes [5].

**A. Wireless sensor network:** In our system, we consider stationary wireless sensor nodes. Each sensor node has only the capacity to report aggregate locations to a server that contains the aggregate query processor. The communication between the sensor nodes and the server is through a distributed tree.

**B. Aggregate query processor:** The aggregate query processor is embedded in the 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.

**C. Resource-efficient sensor scheduler:** We employ a resource-efficient sensor scheduler that aims to reduce the rate of aggregate location information sent from each sensor node to the server. The main idea is that instead of having all sensor nodes send their information to the server at each single time unit, we alternate among the sensor nodes in a round robin fashion. In this case, at each time unit, only a few of the sensor nodes report their aggregate location information to the query processor, so our sensor scheduler can save the sensor energy and network bandwidth [9].

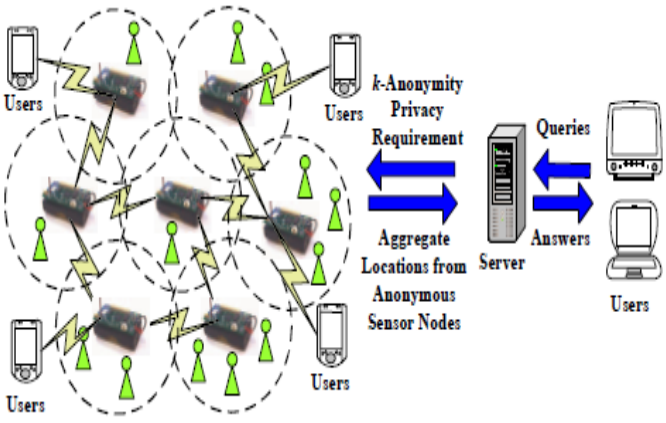



Figure 1: System Architecture

## 3. METHODOLOGY

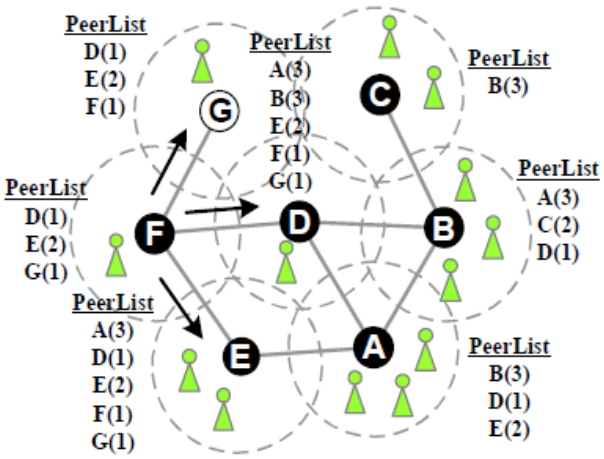
### A. WSN Location Monitoring Module

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.




Rebroadcast from sensor node *F*

### C. Mapped Location monitoring Module

1. **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.

2. **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 anonym zed level k of the system at any time by disseminating a message with a new value of k to all the sensor nodes.

3. **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. Algorithm

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 [10]. 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.

### E. Resource Aware Algorithm

The resource aware algorithm has three major steps, namely, (1) Broadcast step (2) Cloaked area step and (3) Validation step.

**1) Broadcast step:** In this step, every sensor node in a network broadcasts a message which contains id, area and number of nodes to its nearest neighbour. In this way every sensor node forms its own table and also checks for adequate number of objects in its sensing area and accordingly it sends notification message to the nearer sensor nodes and follows the next step.

**2) 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, it uses a greedy approach to find a cloaked area based on the information stored in table. Each sensor node initializes a set S and then determines a score for each peer in its table. The score is defined as a ratio of the object count of the peer to the distance between the peer and node. The score is calculated to select a set of peers from table 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 table to S until S contains at least k objects. Finally, node determines the cloaked area that is a minimum bounding rectangle that covers the sensing area of the sensor nodes in S, and the total number of objects in S.

**3) Validation step:** Validation step is used 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.

**Resource Aware Algorithm**

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

**F. Quality Aware Algorithm**

This algorithm has three steps. (1) Search space step, (2) Minimal cloaked area step and (3) Validation step.

1) **Search space step:** Sensor network has a large number of sensor nodes hence it is very costly for a sensor node to gather the information of all the sensor nodes to compute its minimal cloaked area. To reduce the cost, node determines a search space based on the input cloaked area computed by the resource-aware algorithm.

2) **Minimal cloaked step:** This step takes a collection of peers that live in the search space "S". They are taken as input and computation takes place to find minimum cloaked area for the given sensor. Although search space is pruned for efficiency, all combinations are to be searched. To overcome this problem, two optimization techniques are introduced. The first optimization technique is to verify only four nodes almost instead of all combinations. The other optimization technique has two properties namely monotonicity property and lattice structure. Lattice set is generated to improve search operations while monotonicity is used to reduce the number of objects in the MBR. Afterwards, a progressive refinement is performed for finding minimal cloaked area.

3) **Validation step:** 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.

**Quality 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,.....,aδ+1 } in C[i] do
9. if Area (MBR(X)) < Area (current_min_cloaked_area) then
10. if N(MBR(X))≥ k then
11. current_min_cloaked_area ←{X}
12. Remove X from C[i]
13. end if
14. else
15. Remove X from C[i]
16. end if
17. end for
18. if i<4 then
19. for each itemset pair X = {x1,....xδ+1},
Y = {y1,.....,yδ+1} in C[i] do
20. if x1 = y1,.....,xδ = yδ and xδ+1 ≠ yδ+1 then
21. Add an itemset {x1,.....,xδ+1,yδ+1} to C[i+1]
22. end if
23. end for
24. end if
25. end for
26.Area←a minimum bounding rectangle of current_min_cloaked_area
27.N ←the total number of objects in current_min_cloaked_area
// Step 3: The validation step
28. Lines 18 to 25 in Algorithm 1

## Conclusion:

The proposed framework identifies a Privacy-Preserving Location Monitoring System using wireless sensor network. The estimated distribution is used to provide location monitoring services to answering queries. This proposed system ensures to provide high quality location monitoring services for system users, while preserving personal location privacy. The approach and the concept used in this paper has more broad relevance, can utilize this productive highlights and their applications in all systems administration methods.

## References:

[1] Na Li, Nan Zhang , Saja l K . Das, and Bhavani Thuraisingham, " Privacy preservation in wireless sensor networks: A State -of- the- art survey ", Ad Hoc Networks, vol. 7, pp. 8, pp.1501-1514, April 2009.

[2] Yong Xi, Loren Schwiebert, and Weisong Shi, "Preserving Source location privacy in monitoring-based wireless sensor Networks ", In the proceedings of Parallel and Distributed Processing, no. 1, pp. 8, April 2006.

[3] Chi-Yin Chow, Wenjian Xu and Tian He, "Privacy Enhancing Technologies for Wireless Sensor Networks," © Springer-Verlag Berlin Heidelberg 2014.

[4] D. Culler and M. S. Deborah Estrin, .Overview of sensor networks, IEEE Computer, 2004.

[5] S.T. Birchfield and S. Rangarajan, "Spatiograms Versus Histograms for Region-Based Tracking," Proc. CVPR, June 2005, pp. 1158-1163.

[6] Chi-Yin Chow Mohamed F. Mokbel Tian He. Aggregate Location Monitoring for Wireless Sensor Networks: A Histogram-based Approach. Tenth International Conference on Mobile Data Management: Systems, Services and Middleware 2009.

[7] Y. Li, H. Ai, C. Huang, and S. Lao, "Robust Head Tracking with Particles Based on Multiple Cues," Proc. ECCV Workshop on HCI, 2006.

[8] 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.

[9] Vissamsetti Poorna Surya Vinay Kumar, Kakara Ravi Kumar,. "Location Monitoring algorithms for Wireless Sensor Networks",et al, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 6, November 2012.

[10] M.N.Praneswara Rao, G.Radha Devi, "Resource Aware and Quality Aware Secure Location Monitoring Algorithm for WSNs",. International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 6, December 2012

[11] T. Xu and Y. Cai, .Exploring historical location data for anonymity preservation in location-based services,. in Proc. of Infocom, 2008.

[12] 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.

[13] 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.

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

[15] Mahsa Mirabdollahi Shams, Hojat Kaveh, Reza Safabakhsh. Traffic Sign Recognition using an extended bag-of-features model with Spatial Histogram,. in proc. IEEE, 2015.

[16] Yun Li and Jian Ren. Preserving Source-Location Privacy in Wireless Sensor Networks,.in proc. IEEE Secon 2009.

[17] Usama Salama, Lina Yao, Xianzhi Wang, Hye-young Paik, Amin Beheshti. Multi-Level Privacy-Preserving Access Control as a Service for Personal Healthcare Monitoring,. In proc. IEEE 24th International Conference on Web Services 2017.

[18] Vissamsetti Poorna Surya Vinay Kumar, Kakara Ravi Kumar. Location Monitoring algorithms for Wireless Sensor Networks. International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 6, November 2012.

[19] Francesco Pittaluga Aleksandar Zivkovic Sanjeev J. Koppal. Sensor-level Privacy for Thermal Cameras,. in proc .IEEE 2016.

[20] Arumugam P, Dr.T.Krishna Kumar, Dr.V.Khanna, Dr.J.Sundeep Aanand, Recognizing and Localizing Anamolyfor Wireless Sensor Networks,. International Journal of Pure and Applied Mathematics Volume 118 No. 18 2018.

[21] Soumyasri S M, Rajkiran Ballal. "Novel resource-quality aware algorithm for privacy- preserving location monitoring in wireless sensor networks". 9th International Conference, Edinburgh, United Kingdom, 22nd -23rd July 2017.

[22] Matthew Bradbury, Matthew Leeke and Arshad Jhumka. A Dynamic Fake Source Algorithm for Source Location Privacy in Wireless Sensor Networks,. In proc .IEEE 2015.

[23] Stanley T. Birchfield and Sriram Rangarajan. Spatial Histograms for Region-Based Tracking. ETRI Journal, Volume 29, Number 5, October 2007