Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Location Monitoring System in Wireless Sensor Networks Using Aggregate Query Processor

S. Suresh Kumar[1], Mrs. Manjula.G[2]

[1](MTech Student, Department of ISE, East West Institute of Technology, Karnataka, India,

[2](Assistant Professor, Department of ISE, East West Institute of Technology, Karnataka, India,

Abstract -Monitoring personal locations with a potentially untrusted server poses privacy threats to the monitored individuals. To this end, we propose a privacy-preserving location monitoring system for wireless sensor networks. In our system, we design two in-network location anonymization algorithms, 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 for our system.

Keywords – Aggregate location, Anonymization,Cloaked area, Sensor node, WSN.

I. INTRODUCTION

The advance in wireless sensor technologies has resulted in many new applications for military and/or civilian purposes. 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 sensors or counting sensors. For identity sensors, for example, Bat and Cricket, 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 , and thermal sensors, 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. 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, 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. 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, 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 finds 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.

We evaluate our system through simulated experiments. The results show that the communication and computational cost of the resource-aware algorithm is lower than the quality-aware algorithm, while the quality-aware algorithm provides more accurate monitoring services (the average accuracy is about 90%) than the resource-aware algorithm (the average accuracy is about 75%). Both algorithms only reveal k-anonymous aggregate location information to the server, but they are suitable for different system settings. The resource-aware algorithm is suitable for the system, where the sensor nodes have scarce communication and computational resources, while the quality-aware algorithm is favorable for the system, where accuracy is the most important factor in monitoring services.

II. RELATED WORK

Straightforward approaches for preserving users' location privacy include enforcing privacy policies to restrict the use of collected location information and anonymizing the stored data before any disclosure. However, these approaches fail to prevent internal data thefts or inadvertent disclosure. Recently, location anonymization techniques have been widely used to anonymize personal location information before any server gathers the location information, in order to preserve personal location privacy in location-based services. These techniques are based on one of the three concepts.

A. False Locations

Instead of reporting the monitored object's exact location, the object reports n different locations, where only one of them is the object's actual location while the rest are false locations.

B. Spatial Cloaking.

The spatial cloaking technique blurs a user 's location into a cloaked spatial area that satisfy the user 's specified privacy requirements.

C. Space Transformation.

This technique transforms the location information of queries and data into another space, where the spatial relationship among the query and data are encoded.

In terms of system architecture, existing spatial cloaking techniques can be categorized into centralized, distributed, and peer-to-peer approaches. In general, the centralized approach suffers from the mentioned internal attacks, while the distributed approach assumes that mobile users communicate with each other through base stations is not applicable to the wireless sensor network. Although the peer-to-peer approach can be applied to the wireless sensor network, the previous work using this approach only focuses on hiding a single user location with no direct applicability to sensor-based location monitoring. In the wireless sensor network, Cricket [2] is the only privacy-aware location system that provides a decentralized positioning service for its users where each user can control whether to reveal her location to the system. However, when many users decide not to reveal their locations, the location monitoring system cannot provide any useful services. This is in contrast to our system that aims to enable the sensor nodes to provide the privacy-preserving aggregate location information of the monitored objects. The closest work to ours is the hierarchical location anonymization algorithm [6] that divides the system space into hierarchical levels based on the physical units, for example, sub-rooms, rooms and floors. If a unit contains at least k users, the algorithm cloaks the subject count by rounding the value to the nearest multiple of k. Otherwise, the algorithm cloaks the location of the physical unit by selecting a suitable space containing at least k users at the higher level of the hierarchy. This work is not applicable to some landscape environments, for example, shopping mall and stadium, and outdoor environments. Our work distinguishes itself from this work, as location monitoring services while the usability of anonymized location data was not discussed in [6].

Other privacy related works include: anonymous communication that provides anonymous routing between the sender and the receiver , source location privacy that hides the sender 's location and identity , aggregate data privacy that preserves the privacy of the sensor node's aggregate readings during transmission , data storage privacy that hides the data storage location , and query privacy that avoids disclosing the personal interests . However, none of these previous works is applicable to our problem. The false location techniques cannot provide high quality monitoring services due to a large amount of false location information. The space transformation techniques cannot provide privacy-preserving monitoring services as it reveals the monitored object's exact location information to the query issuer. The spatial cloaking techniques can provide aggregate location information to the server and balance a trade-off between privacy protection and the quality of services by tuning the specified privacy requirements, for example, k-anonymity and minimum area privacy requirements [7], [14]. Thus we adopt the spatial cloaking technique to preserve the monitored object's location privacy in our location monitoring system.

III. System Architecture

A. 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.

B. 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 any time by disseminating a message with a new value of k to all the sensor nodes.

Figure 1 depicts the architecture of our system, where there are three major entities, sensor nodes, server, and system users

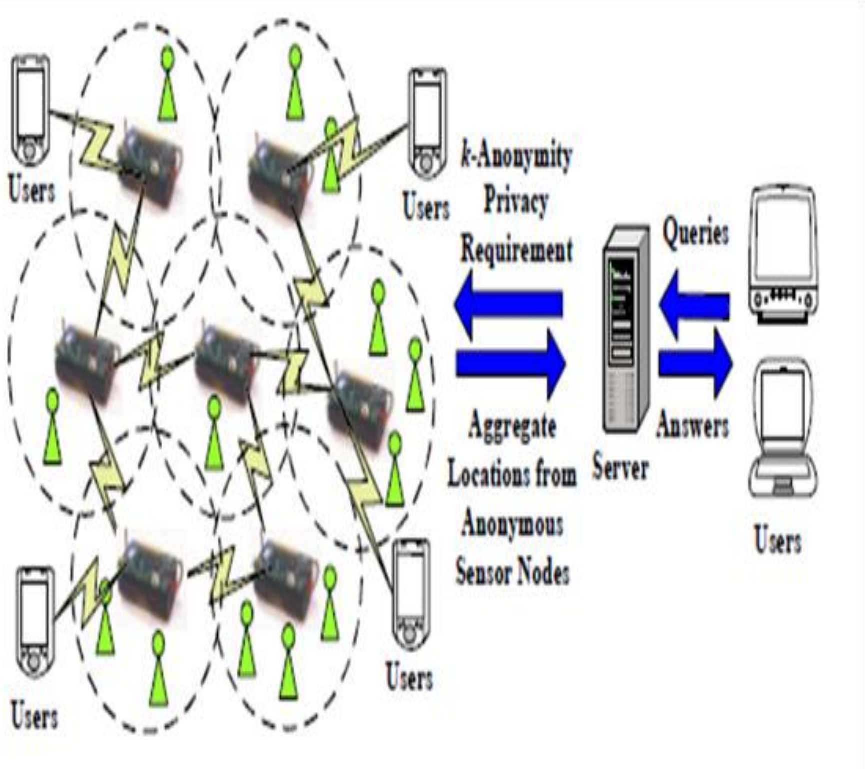
Users
Users
k-Anonymity Privacy Requirement
Aggregate Locations from Anonymous Sensor Nodes
Server
Queries
Answers
Users
Users
Users

Fig 1: System Architecture

C. System User

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

Given a aggregate location R, server only knows that sender of R is one of the sensor nodes with R. Only authenticated administrator can change the k-anonymity level and the spatial histogram cases.Each sensor nodes reports only k-anonymous aggregate location to the server, the adversary cannot infer an objects exact location with an fieldility. Spatial histogram at server provides low quality services for small area and high quality services for large area. This is better privacy-preserving feature

IV. Algorithms

A. The Resource-Aware Algorithm

Algorithm outlines the resource-aware location anonymization algorithm. Figure 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 can communicate with each other directly.

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 con-tainment relationship to the server

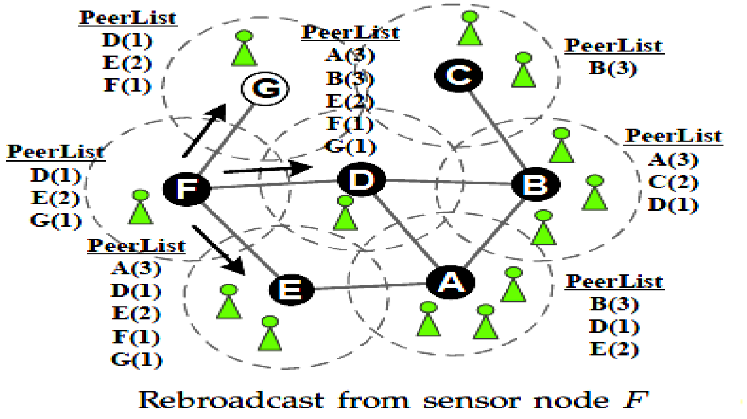

Fig 2: Cloaked Area of Sensor nodes

```
RESOURCEAWARE (Integer k, Sensor m, List R)
// Step 1: The broadcast step
Send a message with m's identity m.ID, sensing area m.Area, and object Count m.Count to m's neighbor peers
if Receive a message from a peer p, i.e., (p:ID, p:Area, p:count) then
    Add the message to PeerList
    if m has found an adequate number of objects then
        Send a notification message to m's neighbors
    end if
    if Some m's neighbor has not found an adequate number of objects then
        Forward the message to m's neighbors
    end if
end if
// Step 2: The cloaked area step
S ←{m}
Compute a score for each peer in PeerList
Repeatedly select the peer with the highest score from PeerList to S until the total number of objects in S is at least k. Area a minimum bounding rectangle of the senor nodes in S N the total number of objects in S
// Step 3: The validation step
if No containment relationship with Area and R 2 R then
    Send (Area, N) to the peers within Area and the Server
else if m's sensing area is contained by some R 2 R then
    Randomly select a R'€ R such that R'.Area contains m's sensing area
    Send R' to the peers within R'.Area and the server
else
    Send Area with a cloaked N to the peers within Area and the server
end if
```

© 2013, IJARCSSE All Rights Reserved

B. Quality Aware Algorithm

The quality-aware algorithm starts from a cloaked area A, which is computed by 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

Step 1: 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 cloaked area computed by the resource-aware algorithm, such that the sensor nodes outside S cannot be part of the minimal cloaked area.

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. In this step 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. Because at most two sensor nodes defines width of MBR and at most two sensor nodes defines height of MBR. Thus this optimization mainly reduces computational cost by reducing the number of MBR computations among the peers in S. The second optimization technique lattice structure and monotonicity property. In a lattice structure, a data set that contains n items can generate 2n-1 item sets excluding a null set. We generate the lattice structure from the lowest level based on a simple generation rule. The monotonicity property of a function f indicates that if X is a subset of Y , then f(X) must not exceed f(Y). For our problem, the MBR of a set of sensor nodes S has the monotonicity property,because adding sensor nodes to S must not decrease the area of the MBR of S or the number of objects within the MBR of S.

Step 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.

```
QUALITYAWARE (Integer k, Sensor
m, Set init solution, List R) current min cloaked
area init solution
// Step 1: The search space step
Determine a search space S based on init solution
Collect the information of the peers located in S
// Step 2: The minimal cloaked area step
Add each peer located in S to C[1] as an item
Add m to each itemset in C[1] as the first item
for i = 1; i ≤4; i ++ do
    for each itemset X = {a1 ,……., ai+1 } C[i] do
        if Area(MBR(X)) < Area(current min cloaked area) then
            if N(MBR(X)) ≥ k then
                current min cloaked area ← {X}
                Remove X from C[i]
            end if
        else
            Remove X from C[i]
        end if
    end for
    if i < 4 then
        for each itemset pair X={x1 ,……, xi+1 } Y ={yi ,….., yi+1 } do
            if x1 = y1 ,…., xi = yi and xi+1 ≠ yi+1 then
                Add an itemset {x1 ,……, xi+1 , yi+1} to C[i + 1]
            end if
        end for
    end if
end for
Area ← a minimum bounding rectangle of current min cloaked area
N ← the total number of objects in current min Cloaked area
// Step 3: The validation step
if No containment relationship with Area and R 2 R then
    Send (Area, N) to the peers within Area and the server
else if m's sensing area is contained by some R 2 R then
    Randomly select a R’€ R such that R’.Area contains m's sensing area
    Send R’ to the peers within R’.Area and the server
else
    Send Area with a cloaked N to the peers within Area and the server
Endif
```

V. Experimental Setup

Above mathematical model can be implemented by using jdk 1.5/1.6 and above and users location is monitored by using j2me which supports wireless toolkit which is Sun Java Wireless Toolkit 2.5.2. Aggregate location of nodes can be shown with the help of maps.

VI. Features Of System

A. WSN Location Monitoring

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 Location

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. 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. Minimum Bounding Rectangle

We find the minimum bounding rectangle (MBR) of the sensing area of sensor node. It is important to note that the sensing area can be in any polygon or irregular shape. MBR’s concept have been wildly adopted by existing query processing algorithms and most database management system have ability to manipulate MBR’s efficiently.

D. Mapped Location Monitoring

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 locatioNand sensing area 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. Authenticated administrators and users can issue range queries to our system through either the server or the sensor nodes, as depicted in above figure 1. The server uses the spatial histogram to answer their queries.

VII. Conclusion

In our paper we proposed a model for privacy preservation of mobile users with the help of anonymization and aggregate location monitoring concept in a wireless sensor network. Two location anonymization algoritms namely resource-aware and quality-aware algoritms are designed to preserve personal location and provide location monitoring services.Sensor nodes execute location anonymization algorithms to provide k-anonymous aggregation location.

Acknowledgment

We would like to take this opportunity to express our gratitude to all those without whose help this project would not have been possible. With all respect and gratitude, firstly, We would like to thank my project guide Asst.Prof. Mrs. Manjula.G who was the driving force behind this project. She guided me at each phase of right through my project giving me priceless advice to improve my modules and websites related to our project.This report is the result of hard work put by my project guide. Finally i utmost thankful to HOD Prof. Dr.Suresh M.B for keeping faith in me. Thanks to Principal, Head, Guide, Co-guide and who so ever helped the student.

References

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

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

[3] 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

[4] 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.

[5] 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.

[6] B. Son, S. Shin, J. Kim, and Y. Her, "*Implementation of the Real-Time People Counting System using Wireless Sensor Networks," IJMUE,vol. 2, no. 2, pp. 63–80, 2007*

http://java.sun.com
http://www.sourcefordgde.com
http://www.networkcomputing.com/
http://www.roseindia.com/
http://www.java2s.com/