Protecting Privacy When Disclosing Information By using Wireless Sensor Networks

P SURYA CHANDRA
M.tech in CSE dept
SVU college of engineering
Tirupati, Andhra Pradesh

RAVI BOLLEDDULA
M.tech in CSE dept
SVU college of engineering
Tirupati, Andhra Pradesh

Abstract— ***The Sensor networks promise to have a significant commercial impact by providing strategic and timely data to new classes of real-time monitoring applications. I proposed two algorithms like, resource aware and quality aware algorithms. Here also to provide high quality location monitoring services for system users. The advantage of this algorithms is to reduce communication cost as well as computational cost and provides high quality monitoring. This both algorithms works on k-anonymity privacy concept. This paper provides a formal model for the source-location privacy problem in sensor networks and examines the privacy characteristics of different sensor routing protocols. The main purposes of Our system is people-counting method can automatically count the number of incoming and outgoing people at a special point in real time. Wireless sensor networks have very broad application prospects including both military and civilian usage Sensor networks have the potential to radically change the way people observe and interact with their environment.***

Keywords: Wireless sensor networks, counting and identity sensors, location monitoring systems

I. Introduction

A Wireless Sensor Network is to be made up of a large number of sensors and at least one base station. The sensors are autonomous small devices with several constraints like the battery power, computation capacity, communication range and memory. They also are supplied with transceivers to gather information from its environment and pass it on up to a certain base station, where the measured parameters can be stored and available for the end user. In most cases, the sensors forming these networks are deployed randomly and left unattended to and are expected to perform their mission properly and efficiently. As a result of this random deployment, the WSN has usually varying degrees of node density along its area.

The Sensors networks are also energy constrained since the individual sensors, which the network is formed with are extremely energy-constrained as well the communication devices on these sensors are small and have limited power and range. Both the probably difference of node density among some regions of the network and the energy constraint of the sensor nodes cause nodes slowly die making the network less dense. Also it is quite common to deploy WSNs in harsh environment, what makes many sensors inoperable or faulty. For that reason, these networks need to be fault-tolerant so that the need for maintenance is minimized. Typically the network topology is continuously and dynamically changing, and it is actually not a desired solution to replenish it by infusing new sensors instead the depleted ones. A real and appropriate solution for this problem is to implement routing protocols that perform efficiently and utilizing the less amount of energy as possible for the communication among nodes. Sensor devices in WSNs monitor the same event and report on them to the base station. Therefore, one good approach is to consider that sensors located in the same region of the network will transmit similar values of the attributes. This fact notices inherent redundancy in the node transmissions that may be used by the routing protocol. Sensor networks need protocols, which are specific data centric, capable of aggregating data and optimizing energy Consumption.

The Classification of Wireless Sensor Network subsection is presented a simple classification of sensor networks based on their mode of functioning and the type of target application. The nodes in Proactive Network sort of network periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest. Hence, they provide a snapshot of the relevant parameters at regular intervals. They are well suited for applications requiring periodic data monitoring. Some known instances of this kind are the LEACH protocol, some improvements on LEACH and PEGASIS, Typical instances of this sort of networks. The nodes of the networks according to this scheme react immediately to sudden and drastic changes in the value of a sensed attribute. The Reactive Networks are well suited for time critical applications. Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines. When the sensors detect the event being monitored (heat, pressure), the event is reported to one of the base stations, which then takes appropriate action (e.g., send a message on the internet or to a satellite). Similarly, wireless sensor networks can use a range of sensors to detect the presence of vehicles ranging from motorcycles to train cars.

II. RELATED WORK

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.

The 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.

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.

To 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.

III. SYSTEM MODEL

The System Design Document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces.

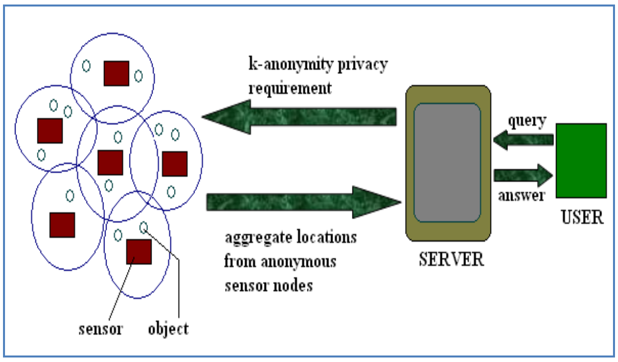

k-anonymity privacy requirement
query
answer
USER
SERVER
aggregate locations from anonymous sensor nodes
sensor
object

Fig. 1: Block diagram of proposed system architecture

DFD

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

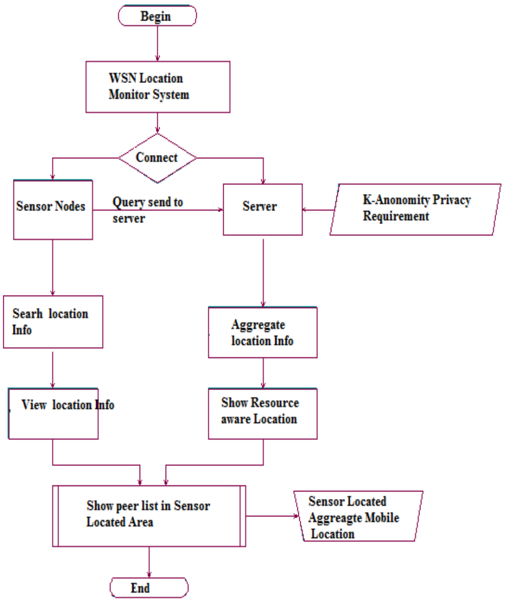

Begin
WSN Location Monitor System
Connect
Sensor Nodes
Query send to server
Server
K-Anonomity Privacy Requirement
Searh location Info
Aggregate location Info
View location Info
Show Resource aware Location
Show peer list in Sensor Located Area
Sensor Located Aggreagte Mobile Location
End

Fig: Data Flow Diagram

LOCATION ANONYMIZATION ALGORITHMS

The proposed location anonymization algorithms are meant for achieving three purposes. The first purpose is that they can enhance the quality of location services. The second purpose is to minimize the computational resources and communication overhead.The third purpose of them is to ensure anonymity of personal location privacy.

Resource – Aware Algorithm

This algorithm is meant for improving resource consumption. It minimizes the computational cost and communication cost while preserving the personal location privacy. The algorithm out line is given in fig. 2.

Algorithm 1 Resurce aware

```
1: function RESOUCEAWARE (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.
```

Fig. 2: Outline of resource – aware algorithm

The resource aware algorithm has three major steps. The first step is known as the broadcast step. In order to minimize the communication and computational cost, this step is aimed at informing all sensor nodes to know required number of objects to be considered in a cloaked area. In the first steps a sensor node sends its ID, sensing area and other details as given in the algorithm to all other sensor nodes. If a sensor receive a message it adds that node in the peer list and sends a message to its neighbors if the node has adequate number of objects. The step2 is cloaked area step in which each sensor node blurs its sensing area into an area known as cloaked area with k objects and k-anonymity is achieved. In order to reduce computational cost, this step also uses a greedy approach. The third step is known as validation step in which it avoids reporting aggregate relationships. Therefore adversaries can't get any information which breaches privacy.

Quality – Aware Algorithm

This algorithm is meant for improving quality of location services. Besides this, it also takes care of location anonymity. The outline of this algorithm is given in fig. 3.

```
Algorithm 2 Quality aware location anonymization
    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
```

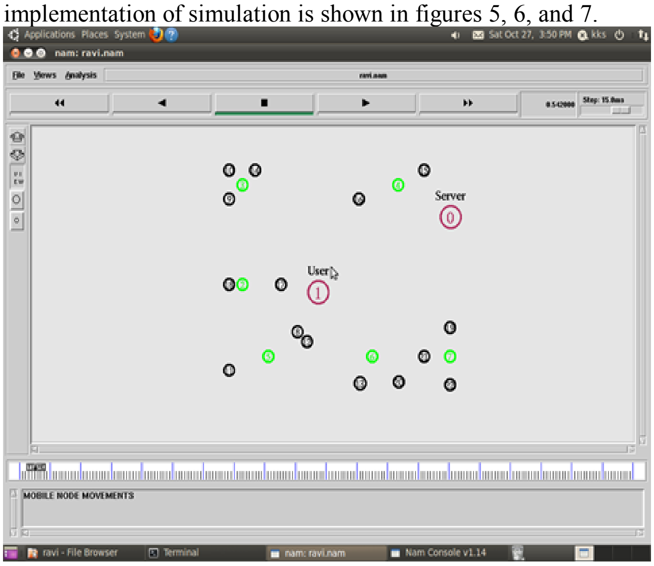
Fig. 3: Quality – aware algorithm

As can be seen in fig. 3, this algorithm has three steps. The first step is known as the search space step. The second step is named the minimal cloaked area step while the third step is known as the validation step. The first step is meant for finding the search space. This is required to reduce communication and computational cost. The step 2 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.

As can be seen in fig. 4, the algorithm outlines the histogram creation and maintenance algorithm that is meant for estimating the distribution of monitored objects.

IMPLEMENTATION

The proposed architectural model and algorithms have been implemented in NS2 that runs in Linux OS. The NS2 implementation of simulation is shown in figures 5, 6, and 7.



As can be seen in fig. 5, the simulation shows sensor nodes, people or objects in movement, user and server. It only shows the movement of sensor nodes and also objects in motion.

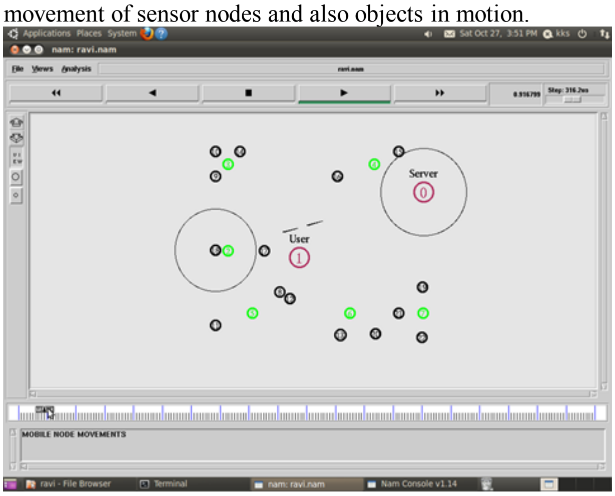
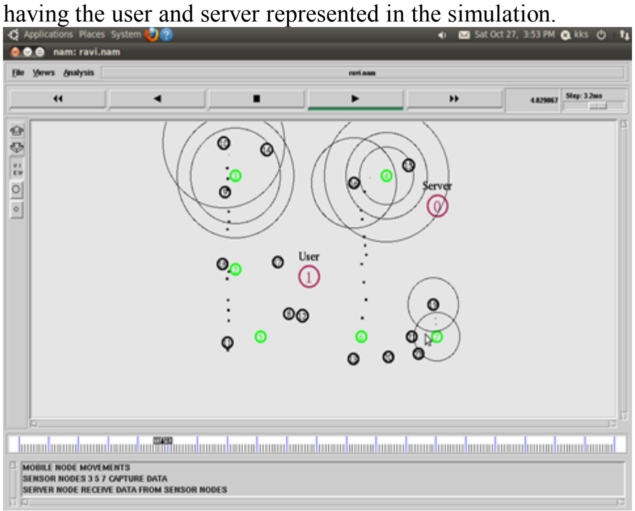


Fig. 6: shows sensor nodes capturing data and sending to server

As can be viewed in the simulation shown in fig. 6, the nodes 3, 5, and 7 are capturing data pertaining to moving objects or people. In the simulation nodes are having their sensing areas marked besides having the user and server represented in the simulation.



MOBILE NODE MOVEMENTS
SENSOR NODES 3 5 7 CAPTURE DATA
SERVER NODE RECEIVE DATA FROM SENSOR NODES

Fig. 7 shows the further simulation of the WSN

As can be viewed in fig. 7, the simulation shows further communication between sensor nodes and the server. The resource-aware and quality-aware algorithms are in place. The system is able to demonstrate the proposed architectural model.

Experimental Results

The experiments made with the simulations using quality – aware and resource – aware algorithms revealed that they are capable of minimizing computational cost and communication cost. At the same time they are able to preserving personal location privacy.

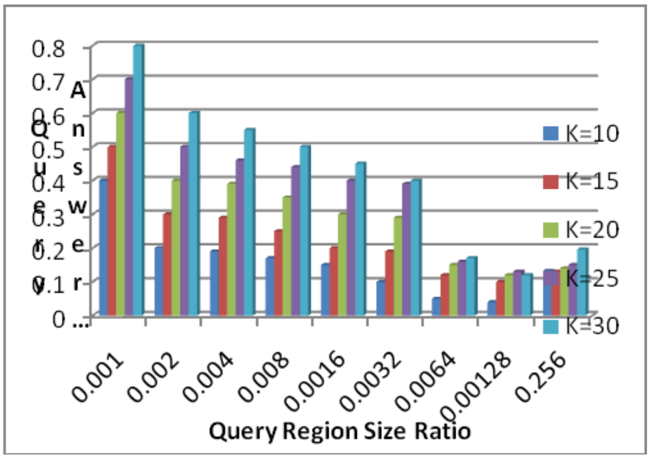


Fig. 8: Resource – aware algorithm

As can be seen in fig. 8, the resource aware algorithm performance is presented. As it is evident in the graph, the more query region size ratio, the less is query answer error. It ensures less computational cost and communication cost.

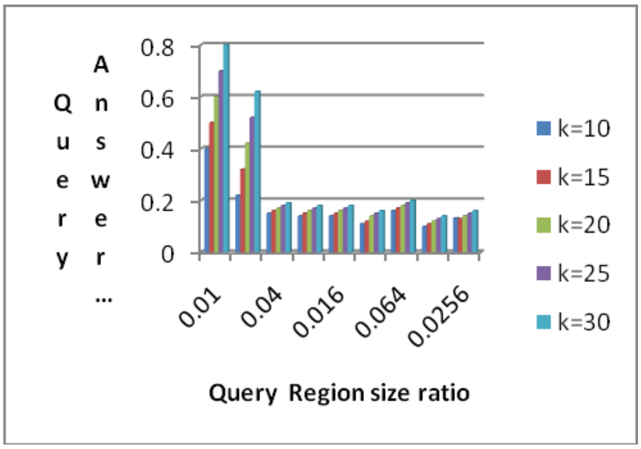


Fig. 9: Quality – aware algorithm

As can be seen in fig. 9, the quality aware algorithm performance is presented. As it is evident in the graph, the more query region size ratio, the less is query answer error. It ensures that the quality of the results is improved.

IV. Conclusion

A privacy-preserving location monitoring system for wireless sensor networks. To 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 in distinguishable 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, to 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. To 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.

References

[1] PandurangKamat, Yanyong Zhang, Wade Trappe, CelalOzturk, 2005 Enhancing Source-Location Privacy in Sensor Network Routing

Available Online at:

http://www.cse.sc.edu/~wyxu/2008-csce790/papers/paris-icdcs2005.pdf

[2] Byung-rak Son, Seung-chan Shin, Jung-gyuKim,Yong-sork Her Implementation of the Real-Time People Counting System using Wireless Sensor Networks

Available Online at:

http://www.sersc.org/journals/IJMUE/vol2_no3_2007/5.pdf

[3]David Culler,Deborah Estrin, ManiSrivastava, 2004, Overview of Sensor Networks

Available online at:

http://compilers.cs.ucla.edu/emsoft05/CullerEstrinSrivastava04.pdf .

[4] Wenbo He,Xue Liu, Hoang Nguyen,KlaraNahrstedt,Tarek Abdelzaher,2007, PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks

Available online at:

http://www.cs.mcgill.ca/~xueliu/Publications/2007_Infocom_PDA.pdf .

[5] Min Shao, Sencun Zhu, Wensheng Zhang, Guohong Cao, Yi Yang, 2009, pDCS: Security and Privacy Support for Data-Centric Sensor Networks
Available online at:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4693710 .

[6] Marco Gruteser, Graham Schelle, Ashish Jain, Rick Han, and Dirk Grunwald, 2003, Privacy-Aware Location Sensor Networks
Available online at:
http://www.winlab.rutgers.edu/~gruteser/papers/2003PrivacyAwareSensors.pdf .

[7] BogdanCarbunar, Yang Yu, Larry Shi, Michael Pearce, VenuVasudevan, 2007, Query privacy in wireless sensor networks
Available online at:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4292832 .

[8] Gabriel Ghinita, PanosKalnis, SpirosSkiadopoulos, 2007, Priv´e**:** Anonymous Location-Based Queries in Distributed Mobile Systems Available Online at:
http://www2007.org/papers/paper223.pdf.

[9] Bu_graGedik, Ling Liu, 2008, Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms
Available online at:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4359010 .

[10] Bhuvan Bamba, Ling Liu, Peter Pesti, Ting Wang,2008, Supporting Anonymous Location Queries in Mobile Environments with Privacy Grid
Available Online at:
http://www2008.org/papers/pdf/p237-bambaA.pdf.

[11] Mohamed F. Mokbel1 Chi Yin Chow 1 Walid G. Aref,2006,The New Casper: Query processing for Location Services without Compromising Privacy
Available online at:
http://infolab.usc.edu/csci587/Fall2010/papers/The%20New%20Casper%20Query%20Processing%20for%20Location%20Services%20without%20Compromising%20Privacy.pdf .