Shiv Sutar, Manjiri Pathak, Prerana Sonawane, Deepali Ugale / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.104-108

Privacy Preservation by Anonymization and Location Monitoring System for WSN

Shiv Sutar*, Manjiri Pathak , Prerana Sonawane***, Deepali Ugale******

*(Department of Computer Science, Pune University, Pune-38)
** (Department of Computer Science, Pune University, Pune-38)
*** (Department of Computer Science, Pune University, Pune-38)
**** (Department of Computer Science, Pune University, Pune-38)

ABSTRACT

Mobile devices are becoming the largest sensor network around the world. They could be used to collect a large amount of data with little effort and cost which is leading to a promising future for sensing networks or urban sensing. Privacy of such mobile users in any areas is very important and critical issue. If Hacker tracks the position of mobile user he can easily access user's personal information and misuse it. To avoid such misuse of confidential data, our system provides privacy through anonymization concept. Anonymization helps user to hide amongst no of users. With the help of anonymization concept we report aggregate location of any user instead of revealing its exact location .Aggregate location monitoring has a simple form of "What is the number of objects in a certain area". Instead of providing exact location of user our system reports group of locations So that an attacker will not be able to track the exact location of user. Along with privacy preservation user's location can also be monitored by our system. Location monitoring is the process of a continuously receiving position that identifies the location for a device or person.

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

1. INTRODUCTION

Wireless sensor network is consists of spatially distributed autonomous sensors to monitor physical or environmental conditions to cooperatively pass their data through the network to a main location in WSN, each user is considered as a node in a network and users are connected through links which are represented as edges on the network.

There are two types of sensors in wireless sensor network: 1.Counting Sensors: These sensors report the count of persons located in their network to a server. 2. Identity Sensors: These type of sensors help system to pinpoint exact location of each monitored person.

There are so many applications running in wireless sensor network. 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.

In our system we are proposing a privacy preservation of such mobile users with the help of anonymization and by reporting aggregate location. An anonymization means a person is indistinguishable amongst k persons in a network. The most effective way to compromise location privacy used by adversary is packet-tracing. In such an attack, an adversary can locate the immediate nodes by eavesdropping the transmitted packet, and further deduce the flow direction of packets. Even worse, the attacker can trace hop-by-hop towards the sink or source nodes. To defend against packet-tracing attack, many approaches are proposed. One of the approaches is providing aggregate location of a user.

Along with privacy preservation of mobile users we are monitoring location of any mobile user through our system. Location monitoring is defined as monitoring every action, movement of any mobile user without disturbing its privacy.

Furthermore in section 2 explains system architecture ,section 3 summerizes implementation and section 4 concludes aim of our system.

2. SYSTEM ARCHITECTURE

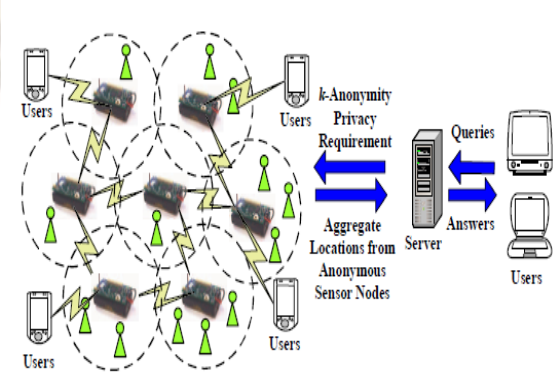

Fig 1: Architecture of system.

System Architecture consists of user, server and trusted zone. There are sensor node and mobile users in a trusted zone .Anonymity level is set by administrator of a system to provide security for mobile users in a trusted zone. The moving objects are shown by green color. What basically happens in a system is a user is asking some query regarding any user in a zone to a server. Server passes this query to a sensor nodes present in trusted zone. Then sensor node from one area will exchange message with the other and report an aggregate location to the server and then server will send the answer to the user.

2.1Problem Definition: To develop a system for privacy preservation and location monitoring for wireless sensor network using location anonymization algorithms.

There are three main entities in our system as sensor node, server and trusted zone. First we will define problem definition of our system and then we will describe the working of entities in detail.

2.1.1 Sensor Node*:* There are various sensor nodes present in a trusted zone. The job of Sensor nodes is to calculate moving objects in its own area. Sensor nodes are anonymous in nature. Sensor nodes communicate with the other sensor nodes to form a peer list by broadcasting a message. After a peer list sensor nodes forms a cloaked area in which there should be k no of objects present. The cloak area is the blurred area which can't b seen by other sensor nodes. That cloaked area is the final aggregate location which is provided to a user through a server.

2.1.2 Server *:* Server can be called as central node as every sensor node is connected to it. Server keeps information about all sensor nodes. Server can be called as communication medium between user and trusted zone i.e. sensor nodes. User first sends a query to a server and then server passes it to sensor nodes.

2.1.3Trusted zone*:* trusted zone consist of several nodes as mentioned earlier. This zone is called as trusted because the anonymous sensor nodes are present in it. Anonymous nature of sensor nodes helps hiding from other senor nodes.

3. PROPOSED SYSTEM MODEL

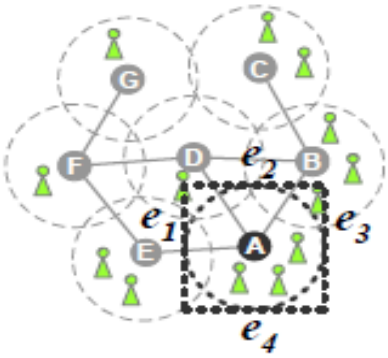

Fig 2: Cloaked Area for Sensor node A

Given a set of sensor nodes S={s1,s2,……..sn} with sensing areas A={a1,a2……an} respectively, a set of moving objects O={o1, o2…….. Om},a set of cloaked areas C={c1,c2……cn},Required anonymity level k, aggregate location for each sensor node si in a form of Ri = (Areai , Ni), where **Areai** is a rectangular area containing the sensing area of a set of sensor nodes Si.

Ni is the number of objects residing in the sensing areas of the sensor nodes in Si,

such that Ni >= k,Ni = j [Usj ε Si Oj] >= k,Oj = {ol / ol ε a},1<= i <= n, and 1 <= l<=m.

4. ALGORITHMS

To implement our system two algorithms are used:

4.1 Resource aware algorithm

Basic idea of this algorithm is to find adequate number of persons in that network and accordingly finding a cloaked area which further referred as MBR(minimum bounded area).there are two steps in this algorithm :

4.1.1 Broadcast step:

In this step, Every sensor node in a network broadcasts a message to nearer sensor nodes.in this message it passes its id,its sensor area and count of objects in its sensing area.In this way every sensor node forms its own peerlist.also every sensor node 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.

4.1.2 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, this step uses a greedy

approach to find a cloaked area based on the information stored in PeerList. For each sensor node m, m initializes a set S and then determines a score for each peer in its PeerList . The score is defined as a ratio of the object count of the peer to the distance between the peer and m. The score is calculated 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 . 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).

4.1.3 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.

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

4.2 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.

4.2.1 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.

4.2.2 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 atmost 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 has two properties, lattice structure and monotonicity property. In a lattice structure, a data set that contains n items can generate 2^{n-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.

4.2.3 The 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.

. **function** 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 = {a_1 ,……., a_{i+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={x_1 ,……, x_{i+1} }
Y ={y_i ,….., y_{i+1} } **do**
if x1 = y_1 ,…., x_i = y_i and $x_{i+1} \neq y_{i+1}$ then
Add an itemset {x_1 ,……, x_{i+1} , y_{i+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
end if

5. 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.

6. FEATURES OF SYSTEM

6.1 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.

6.2 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.

6.3 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.

7 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 aggregate locations.

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 Prof. Shiv Sutar who was the driving force behind this project. He guided us at each phase of us right through our project giving us priceless advice to improve our modules and websites related to our project.This report is the result of hard work put by our project guide. Finally We are utmost thankful to HOD Prof. Rajneeshkaur Bedi for keeping faith in us.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.