INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

AGGREGATE LOCATION MONITORING SYSTEM FOR WIRELESS SENSOR NETWORKS

Bravim J. Jorewar[1], A. S. Alvi[2]

[1]M.E.(I.T.) Scholar Departmet of I.T. [2]HOD, Department of I.T.
[1]PRMIT&R, Badnera, Amravati, India [2]PRMIT&R, Badnera, Amravati, India
[1]bravimjorewar98@gmail.com, [2]abrar_alvi@gmail.com

Abstract- *Supervising private locations with a potentially delegate server pose privacy intimidation to the monitored individuals. To this end, we propose a privacy-preserving location Supervising system for wireless sensor networks. In our system, we design in network location anonymization algorithm namely, resource-aware algorithm that aim to enable the system reaching up to superiority location monitoring services for system users, while preserving individual location privacy. Algorithm relies on the well renowned k-anonymity privacy concept that is a person is identical among k persons to enable trusted sensor nodes to provide the aggregate location in order of supervise persons for our system. Each aggregate position is in a form of a monitored area A along with the number of monitored persons residing in A, where A encloses at least k persons. The resource-aware algorithm aims to minimize consultation cost. To utilize the aggregate location in order to provide location monitoring services, we use an emerge that estimates the distribution of the monitored persons based on the congregate aggregate location information. Then the estimated distribution is used to provide location monitoring services through answering range queries. Coordination shows that our system provides high worth location monitoring services for system users and guarantees the location privacy of the monitored persons.*

Keywords *– Wireless sensor network, Location privacy, Aggregate location, k-anonymity*

1. INTRODUCTION

Privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services. Necessitate each person is identical together with k persons our system relies on the well recognized k-anonymity privacy perception. A smaller k indicates less privacy protection, because a smaller covered area will be reported from the sensor node; hence superior monitoring services. However, a larger k results in a larger cloaked area, which will reduce the quality of monitoring services, but it provides better privacy fortification. Our system can avoid the privacy outflow in the example given in Fig.1 by providing low quality location monitoring services for small region that the enemy could use to track users, while providing high quality services for larger areas. The definition of a small area is relative to the required anonymity level, because our system provides superior quality services for the same area if we relax the required anonymity level [1].

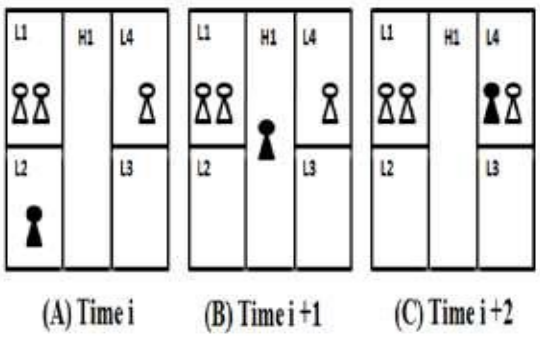

Figure 1: Using counting sensor a location monitoring System

Thus the enemy cannot infer the number of persons currently residing in a small area from our system output with any fidelity. To conserve personal location privacy we propose in-network aggregate location anonymization algorithms namely. Algorithms require the sensor nodes to collaborate with each other to blur their sensing areas into shrouded areas, such that each shrouded area contains at least k persons to constitute a k-anonymous shrouded area [13].The resource-aware algorithm aims to minimize communication cost to the server, but they are suitable for different system settings, each sensor node finds an sufficient number of persons, and then it uses a ravenous approach to find a shrouded area. Then A will be iteratively sophisticate based on extra communication among the sensor nodes until its area reaches the minimal possible size. For the algorithms, the sensor node reports its cloaked area with the number of monitored persons in the area as an aggregate location to the server [1][3]. Even though our system only knows the aggregate location information about the monitored persons, it can still provide monitoring services through answering aggregate queries. The counting sensors in nature they provide aggregate location information, they also produce privacy breach Figure 1 gives an example of privacy breach in counting sensor of an location monitoring system. There are 5 counting sensor nodes given in a lab L1 to L4 and hall H1 Fig1. There are non zero number of persons sense by each sensor node. Fig.1.B and 1C has a sensor node at two time case Ti+1 and Ti+2 that give the number description by each sensor node. If L2 is John lab an enemy knows that John is in lab L2 at Ti. Then enemy knows that John left L2 at time Ti+1 and went to H1 by

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

knowing the number of persons sense by sensor node in H1 and L2. Same, enemy knows that John left H1 at Ti+2 and went to L4. So, privacy breach occurs, so it may lead to an privacy threats. Similarly we can also know that a person has visited restaurant in mall building. To afford monitoring services, we proposes implementing privacy preserving location monitoring system in WSN consists of a k anonymity privacy perception [4][13].

2. OBJECTIVE

Input Design is the process of converting a user-oriented explanation of the input into a computer-based system. This mean is important to keep away from errors in the data input procedure and show the precise direction to the management for getting precise information from the computerized system. It is accomplish by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to create data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data influence can be performed. It also provides evidence viewing facilities. When the data is entered it will ensure for its validity. Data can be entered with the help of screens. Suitable messages are provided as when needed so that the user will not be in maize of on the spot.

3. SYSTEM MODEL

3.1 Sensor nodes.

Each sensor node is responsible for decisive 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 cooperative location information to the server. We do not have any postulation 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[1][4][7].

3.2 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. moreover, the administrator can change the anonymzed level k of the system at anytime by disseminating a message with a new value of k to all the sensor nodes.

3.3 System users:

Legitimate administrators and users can issue range queries to our structure through either the server or the sensor nodes, as depicted in Fig 2. The server uses the spatial histogram to answer their queries[2][8].

3.3 Privacy model:

In our system, the sensor nodes comprise a trusted zone, where they perform as defined in our algorithm and converse with each other through a secure network channel to avoid internal network attacks, for example, eavesdropping, traffic analysis, and malevolent nodes . Since establishing such a secure network channel has been studied in the prose, the discussion of how to get this network channel is away from the scope of this paper. However, the solutions that have been used in previous works can be applied to our system. Our system also provides anonymous communication between the sensor nodes and the server by employing existing anonymous announcement techniques. Thus given an aggregate location R, the server only knows that the sender of R is one of the sensor nodes within R. Moreover, only authenticated administrators can change the k-anonymity level and the spatial histogram size. In emergency cases, the administrators can set the k-anonymity level to a small value to get more precise collective locations from the sensor nodes, or even set it to zero to disable our algorithm to get the original readings from the sensor nodes, in order to get the best services from the system [9]. Since the server and the system user are outside the trusted zone, they are entrusted.

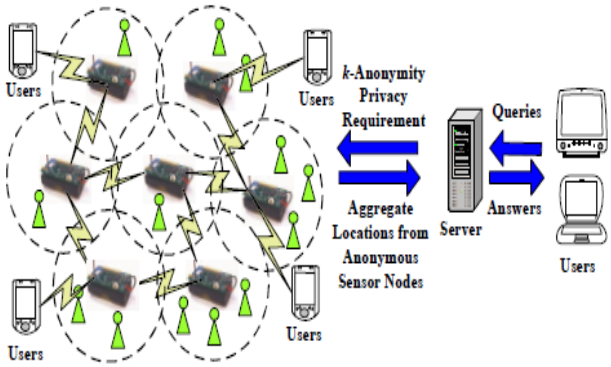

Figure 2: Proposed Architecture

We now confer the privacy hazard in existing location monitoring systems. In an identity-sensor position monitoring system, since each sensor node reports the exact location information of each monitored object to the server, the opponent can pinpoint each object's correct location. On the other hand, in a counting-sensor location monitoring system, each sensor node reports the number of objects in its sensing area to the server. The opponent can map the monitored areas of the sensor nodes to the system layout[12]. If the object count of a monitored area is very small or equal to one, the opponent can infer the identity of the monitored objects based on the mapped monitored area. The larger the anonymity level, k, the more tricky for the opponent to infer the object's exact location[5].With the k-anonymzed aggregate locations reported from the sensor nodes, the underlying spatial histogram at the server provides low quality location monitoring services for a small area, and better quality services for larger areas. This is a amusing privacy-preserving feature, because the object count of a small area is more likely to reveal personal location information. The definition of a small area is relative to the required anonymity level, because our system provides lower quality services for the same area if the anonymzed level gets stricter. We will also describe an attack model, where we arouse an attacker that could be a system user or the server attempting to infer the object count of a particular sensor

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

node. We evaluate our system's flexibility to the attack model and its privacy fortification [4][13] .

4. PROCESS SPECIFICATION

4.1 Input design:

The input design is the link between the information system and the user. It comprises the developing specification and events for data training and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can happen by having people keying the data directly into the system. The design of input focuses on controlling the quantity of input required, controlling the errors, avoiding impediment, avoiding extra steps and keeping the process simple[3][10]. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur**.**

4.2 Output design:

A superiority output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system throughout outputs. In output design it is determined how the information is to be displaced for instantaneous need and also the hard copy output. It is the most important and direct source information to the user. proficient and intelligent output design improves the system's relationship to help user decision-making[3][4].

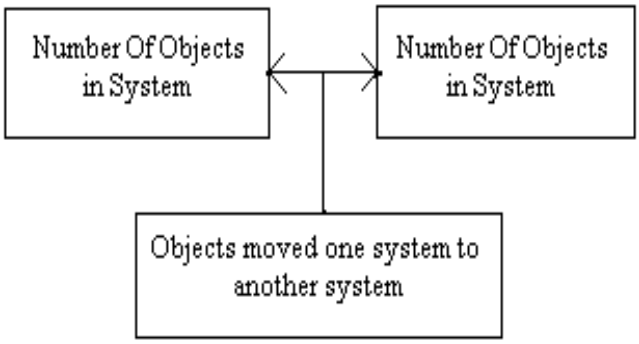

Figure 3: Steps in resource aware algorithm

Designing computer output should ensue in an prepared, well thought out approach; the right output must be developed while ensuring that each output element is designed so that people will discover the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements. Choose methods for presenting information. Create document, report, or other formats that contain information formed by the system. The output form of an information system should accomplish one or more of the following objectives.

- Express information about past activities, current status or projections of the
- Prospect.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

4.3 Technique resource-aware algorithm:

The resource-aware algorithm aims to reduce communication and computational cost. Then A will be iteratively efficient based on extra communication with the sensor nodes until its area reaches the minimal possible size. For algorithm the sensor node information its cloaked area with the number of monitored persons in the area as an aggregate location to the server. To avoid reporting aggregate locations with a suppression relationship to the server validation is required. We do not allow the sensor nodes to report their aggregate locations with the suppression relationship to the server, because combining these aggregate locations may pose privacy escape. 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 negligible shrouded area [1]. To reduce the cost, node determines a search liberty based on the input cloaked area computed by the resource-aware algorithm. To propose location monitoring services based on the aggregate location information, we recommend a spatial histogram move toward 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 [6]. We evaluate our system through replicated experiments. Information of all the sensor nodes to compute its minimal cloaked area. To trim down the cost, node determines a search space based on the input cloaked area computed by the resource-aware algorithm. 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 offer location monitoring services through answering range queries[11][12].

5. CONCLUSION AND FUTURE SCOPE

In this paper, propose an efficient location tracking system and we explained anonymization algorithms namely resource aware algorithm and we efficiently track the client and the path of the files. To minimize communication and computational cost resource aware algorithm used. While preserving the monitored object's location privacy, the results supporting statement that high quality monitoring services. Our system is good for location privacy preserving monitoring system because the area is large then the attacker cannot find out exact location.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

REFERENCES

[1]C Chow, M. Mokbel, T. He, "A Privacy Preserving Location Monitoring System using Wireless Sensor Network", vol. 10, No.1,January 2011 .

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

[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]Dattatray P. Gade, Dhiraj S. Rathod, Vilas R. Khomne, Yogita R. Avhad Pune University "Implementing Privacy Preserving Location Monitoring System in WSN" Volume 3, Issue 3, March 2013.

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

[6] G. Kaupins and R. Minch,"Legal and ethical implications of employee location monitoring" in Proc. of HICSS, 2005.

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

[8] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar,"SPINS: Security protocols for sensor networks". in Proc. of MobiCom,2001.

[9] J. Kong and X. Hong,"ANODR: Anonymous on demand routing with untraceable routes for mobile adhoc networks". in Proc. Of MobiHoc, 2003.

[10] E. Snekkenes, .Concepts for personal location privacy policies, in Proc. of ACM EC, 2001.

[11] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression",. IJUFKS, vol. 10, no. 5, pp. 571.588, 2002.

[12] S. Suresh Kumar[1], Mrs. Manjula.G[2], "Location Monitoring System in Wireless Sensor Networks Using Aggregate Query Processor" Volume 3, Issue 5, May 2013 ISSN: 2277 128X.

[13] Gayathri M ,Bharathi M ,"A K-Anonymity Privacy Preserving Location Monitoring System for Wireless Sensor Networks with Nymble Secure System" International Journal of Computer & Organization Trends –Volume2Issue2- 2012 .