

Privacy Preserving Location Monitoring System for Wireless Sensor Network Algorithm

¹M. A. Ahmedsha, ²M. M. Balakrishna

^{1,2}Dept. of CSE, A.S.R College of Technology, Kakinada, Tadepalligudem, AP, India

Abstract

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. In this paper, we propose a privacy-preserving location monitoring system for wireless sensor networks. 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 with the number of monitored objects, N , located in A , where $N \geq k$, 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.

Keywords

Location Monitoring, Wireless Sensor Network, Location Privacy

I. Introduction

A Wireless Sensor Network (WSN) is a heterogeneous network composed of a large number of tiny low-cost devices, denoted as nodes (or motes), and one or few general purpose computing devices referred to as base stations (or sinks). A general purpose of the WSN is to monitor some physical phenomena (e.g., temperature, barometric pressure, light) inside an area of deployment. Nodes are equipped with a communication unit (e.g., radio transceiver), processing unit, battery and sensor(s). Nodes are constrained in processing power and energy, whereas the base stations have laptop capabilities and not severely energy resources. The base stations usually act as gateways between the WSN and other networks (e.g., Internet).

Wireless sensor network 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:

- Counting Sensors: These sensors report the count of persons located in their network to a server.
- 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.

II. System Architecture

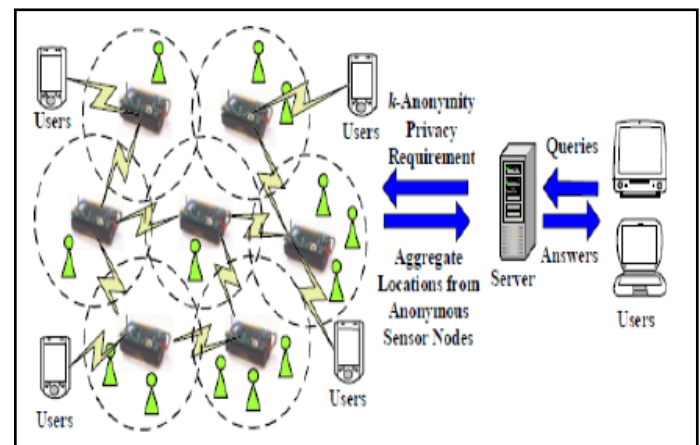


Fig. 1: System Architecture

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.

Problem 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. **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 be seen by other sensor nodes. That cloaked area is the final aggregate location which is provided to a user through a server. Second 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.

Third: Trusted 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 sensor nodes.

III. Proposed System Model

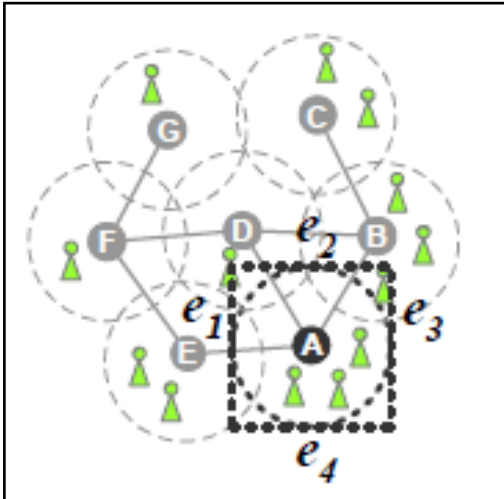


Fig. 2: Cloaked Area for sensor node A

Given a set of sensor nodes $S = \{s_1, s_2, \dots, s_n\}$ with sensing areas $A = \{a_1, a_2, \dots, a_n\}$ respectively, a set of moving objects $O = \{o_1, o_2, \dots, o_m\}$, a set of cloaked areas $C = \{c_1, c_2, \dots, c_n\}$, Required anonymity level k , aggregate location for each sensor node s_i in a form of $R_i = (Area_i, N_i)$, where $Area_i$ is a rectangular area containing the sensing area of a set of sensor nodes S_p . N_i is the number of objects residing in the sensing areas of the sensor nodes in S_p , such that $N_i \geq k, N_i = j [U_{sj} \in S_i O_j] \geq k, O_j = \{o_l / o_l \in a\}, 1 \leq i \leq n$, and $1 \leq l \leq m$.

A. 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:

1. Broadcast

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.

2. Cloaked Area

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).

3. Validation

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.

Algorithm 1 Resource-aware location anonymization

```

1: function RESOURCEAWARE (Integer  $k$ , Sensor  $m$ , List  $R$ )
2: PeerList  $\leftarrow \{\emptyset\}$ 
   // Step 1: The broadcast step
3: Send a message with  $m$ 's identity  $m.ID$ , sensing area  $m.Area$ , and object count  $m.Count$  to  $m$ 's neighbor peers
4: if Receive a message from a peer  $p$ , i.e., ( $p.ID$ ,  $p.Area$ ,  $p.count$ ) then
5:   Add the message to PeerList
6:   if  $m$  has found an 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 neighbors
11:   end if
12: end if
   // Step 2: The cloaked area step
13:  $S \leftarrow \{m\}$ 
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  $S$  is at least  $k$ 
16: Area  $\leftarrow$  a minimum bounding rectangle of the sensor nodes in  $S$ 
17:  $N \leftarrow$  the total number of objects in  $S$ 
   // Step 3: The validation step
18: if No containment relationship with Area and  $R \in R$  then
19:   Send (Area,  $N$ ) to the peers within Area and the server
20: else if  $m$ 's sensing area is contained by some  $R \in R$  then
21:   Randomly select a  $R' \in R$  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

```

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.

1. Search Space

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.

2. The Minimal Area

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 has two properties, 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 .

3. Validation

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.

Algorithm 2 Quality-aware location anonymization

```

1: function QUALITY_AWARE (Integer  $k$ , Sensor  $m$ , Set  $init\_solution$ , List  $R$ )
2:    $current\_min\_cloaked\_area \leftarrow init\_solution$ 
   // 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  $i = 1; i \leq 4; i++$  do
8:     for each itemset  $X = \{a_1, \dots, a_{i+1}\}$  in  $C[i]$  do
9:       if  $Area(MBR(X)) < Area(current\_min\_cloaked\_area)$  then
10:        if  $N(MBR(X)) \geq k$  then
11:           $current\_min\_cloaked\_area \leftarrow X$ 
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  $X = \{x_1, \dots, x_{i+1}\}, Y = \{y_1, \dots, y_{i+1}\}$  in  $C[i]$ 
20:       do
21:         if  $x_1 = y_1, \dots, x_i = y_i$  and  $x_{i+1} \neq y_{i+1}$  then
22:           Add an itemset  $\{x_1, \dots, x_{i+1}, y_{i+1}\}$  to  $C[i+1]$ 
23:         end if
24:       end for
25:     end if
26:   end for
27:    $Area \leftarrow$  a minimum bounding rectangle of  $current\_min\_cloaked\_area$ 
28:    $N \leftarrow$  the total number of objects in  $current\_min\_cloaked\_area$ 
   // Step 3: The validation step
28:   Lines 18 to 25 in Algorithm 1

```

IV. 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 algorithms namely resource-aware and quality-aware algorithms are designed to preserve personal location and provide location monitoring services. Sensor nodes execute location anonymization algorithms to provide k -anonymous aggregate locations.

References

- [1] D. Culler, 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, D. Grunwald, "Privacy-aware location sensor networks", in Proc. of HotOS, 2003.
- [3] W. He, X. Liu, H. Nguyen, K. Nahrstedt, T. Abdelzaher, "PDA: Privacy-preserving data aggregation in wireless sensor networks", Proc. of Infocom, 2007.
- [4] C.-Y. Chow, M. F. Mokbel, 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, 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, Y. Her, "Implementation of the Real-Time People Counting System using Wireless Sensor Networks", IJMUE, Vol. 2, No. 2, pp. 63-80, 2007.
- [7] M. Gruteser, D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking", in Proc. Of MobiSys, 2003.



Mr. M.A. Ahmedsha is a student of Sri Akula Sriramulu college of Technology, Tadepalligudem presently doing his M.Tech (C.S.E) from this college and he received his Bachelor degree from JNTU, Hyderabad. His area of interest is Computer Networks, Database Management System and C-Programming.



MR. M.M. Bala Krishna an efficient faculty member who received his M.Tech in CSE from JNTU and working as Head of the Department in Dept. of CSE in ASR College of Technology, Tadepalligudem. He has 5 years of experience. He Published the papers in international and national journals. His area of interest is Network Programming, Database Management System.

Database Management System.