International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 2, Issue 3(March 2013), PP.01-06
www.irjes.com

Improving High Quality Privacy Preserving Location Monitoring System For Wireless Sensor Networks

1 . Ms. Badi Alekhya.,
[1]*Assistant Professor, T.J.S Engineering College, Department of Computer Science and Engineering*

Abstract: *- . Message authentication is an important objective of information security in modern wireless networks. This objective is met by providing the receiver of the message an assurance of the sender's identity. Digital tools have been developed using cryptography. A major limitations of all cryptographic methods for message authentication lies in their uses of algorithms with fixed symmetric or public keys.This project presents a synchronized random key generation for each node which depends on the position. So there is no need any exact location data to transfer. Key generation protocol is used here. Key generation protocol depends on the global Positioning method. Pseudo random number creation depends upon the position and the initial value of linear feedback shift register. So each and every second create a new key. So the level of privacy information security is too high and power consumption is very low.*

1. 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, [4], and thermal sensors [5], are deployed to report the number of persons located in their sensing areas to a server.
Fig. 1 gives an example of a privacy breach in a location of the monitoring system with counting sensors. There are the11 counting sensor nodes installed in nine rooms R1 to R9, and two hallways C1 and C2 (Fig. 1a). The nonzero number of persons detected by each sensor node is depicted as a number in parentheses. Figs. 1b and 1c give the numbers reported by the same set of sensor nodes at two consecutive time insistanstancesti+1 and ti+2, respectively. If R3 is Alice's office room, an adversary knows that Alice is in room R3 at time ti. Then, the adversary knows that Alice left R3 at time ti+1 and went to C2by knowing the number of persons detected by the sensor nodes in R3 and C2. Likewise, the adversary can infer that Alice left C2 at time ti+2 and went to R7. Such knowledge leakage may lead to several privacy threats. For example, knowing that a person has visited certain clinical rooms may lead to knowing her health records. Also, knowing that a person has visited a certain bar or restaurant in a mall building may reveal confidential personal information.

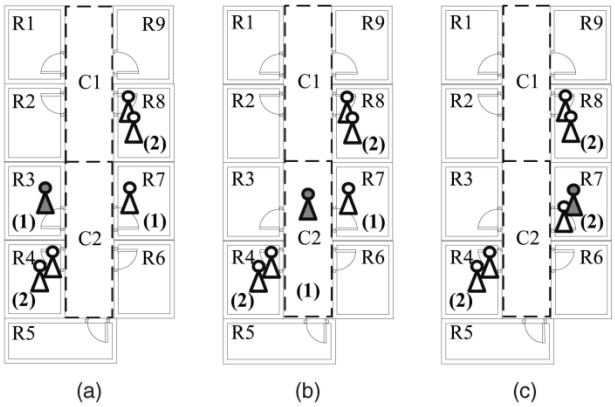


Fig1. A location monitoring system using counting sensors. (a) At time ti. (b) At time ti+1. (c) At time ti+2.

2. 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. How-

ever, these approaches fail to prevent internal data thefts or inadvertent disclosure. Recently, location anonymization techniques have been widely used to anonymize personal location infomation before any server to 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.

1)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

2) Spatial cloaking.

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

3) 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 .Among these three privacy concepts, only the spatial cloaking technique can be applied to our problem. The main reasons for this are that 1) the false location techniques cannot provide high-quality monitoring services due to a large amount of false location information, 2) 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. Thus, we adopt the spatial cloaking technique to preserve the monitored object's location privacy in our location monitoring system.

3.ALGORITHMS

LOCATION ANONYMIZATION ALGORITHMS

In this section, we present our in-network resource and quality-aware location anonymization algorithms, that is.periodically executed by the sensor nodes to report their k-anonymous aggregate locations to the server for every reporting period.

3.1 The Resource-Aware Algorithm

Algorithm 1.
Resource-aware location anonymization
1: function RESOURCEAWARE (Integer k, Sensor m,
List R)
2: PeerList <-{0}
// 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 neighbour 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 neighbours
8: end if
9: if Some m's neighbour has not found an adequate number of objects then
10: Forward the message to m's neighbours
11: end if
12: end if
// Step 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 is at least k
16: Area a minimum bounding rectangle of the senor
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 2 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 2 R then
21: Randomly select a R0 2 R such that R0:Area contains m's sensing area
22: Send R0 to the peers within R0:Area and the server
23: else
24: Send Area with a cloaked N to the peers within Area and the server
25: end if

3.2 Quality-aware location anonymization algorithm

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 C½1_ as an item
6: Add m to each item set in C½1_ as the first item
7: for i ¼ 1; i _ 4; i ++ do
8: for each item set X ¼ fa1; . . . ; aiþ1g in C½i_ 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 C½i_
13: end if
14: else
15: Remove X from C½i_
16: end if
17: end for
18: if i < 4 then
19: for each item set pair X ¼ fx1; . . . ; xiþ1g,
Y ¼ fy1; . . . ; yiþ1g in C½i_ do
20: if x1 ¼ y1; . . . ; xi ¼ yi and xiþ1 6¼ yiþ1 then
21: Add an item set fx1; . . . ; xiþ1; yiþ1g
to C½i þ 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

4. System Architecture

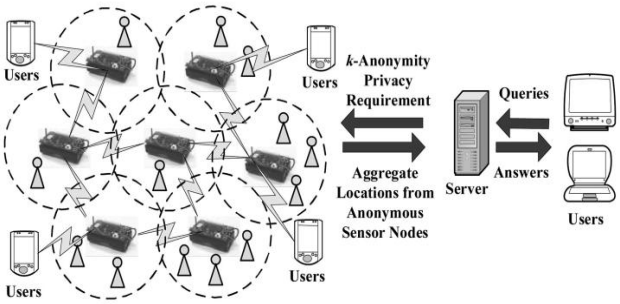


fig2.System Architecture

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 then network topology, as our system only requires a communication path from each sensor node to the server through a distributed tree [10]. Each sensor node is also aware of its location and sensing area.

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 anytime by disseminating a message with a new value of k to all the sensor nodes.

System users:

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

Privacy model:

In our system, the sensor nodes constitute a trusted zone, where they behave as defined in our algorithm and communicate with each other through a secure network channel to avoid internal network attacks, for example, eavesdropping, traffic analysis, and malicious nodes. Since establishing such a secure network channel has been studied in the literature the discussion of how to get this network channel is beyond 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 communication techniques. Thus given an aggregate location R, the server only knows that the sender of R is one of the sensor nodes within R.Furthermore,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 accurate aggregate 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. Since the server and the system user are outside the trusted zone, they are untrusted.We now discuss the privacy threat in existing location monitoring systems. In an identity-sensor location monitoring system, since each sensor node reports the exact location information of each monitored object to the server, the adversary can pinpoint each object's exact 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 adversary can map the monitored areas of the sensor nodes to the system layout. If the object count of a monitored area is very small or equal to one, the adversary can infer the identity of the monitored objects based on the mapped monitored area,

Performance Metrics

We evaluate our system in terms of five performance metrics.

1. Attack model error. This metric measures the resilience of our system to the attacker model by the relative error between the estimated number of objects b N in a sensor node's sensing area and the actual one N. The error is measured as |N-N|/N. When N=0, we consider N^ as the error.

2. **Communication cost**. We measure the communication cost of our location anonymization algorithms in terms of the average number of bytes sent by each sensor node per reporting period. This metric also indicates the network traffic and the power consumption of the sensor nodes.

3. Cloaked area size. This metric measures the quality of the aggregate locations reported by the sensor nodes.The smaller the cloaked area,the better the accuracy of the aggregate location.

4. Computational cost. We measure the computational cost of our location anonymization al gorithms in terms of the average number of the MBR computations that are needed to determine a resource or quality-aware cloaked area. We compare our algorithms with a basic approach that computes the MBR for each combination of the peers in the required search space to find the minimal cloaked area. The basic approach does not employ any optimization techniques proposed for our quality-aware algorithm.

5. Query error. This metric measures the utility of our system, in terms of the relative error between the query of the answer M^, which is the estimated number of objects within the query region based on a spatial histogram, and the actual answer M,respectively.The error is measured as |M^-M|/M When M = 0, we consider M^ as the error.

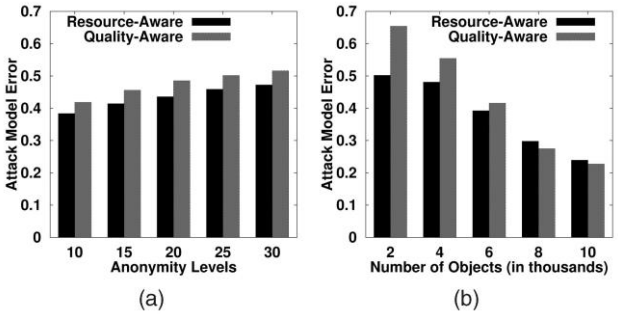
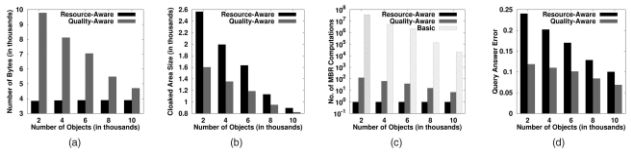


Fig Attacker model error. (a) Anonymity levels. (b) Number of objects

Effect of the Number of Objects

Fig. depicts the performance of our system with respect to the increasing the number of objects from 2,000 to 10,000. Fig. shows that when the number of objects increases, the communication cost of the resource-aware algorithm is only slightly affected, but the quality-aware algorithm significantly reduces the communication cost. The broadcast step of the resource-aware algorithm effectively allows each sensor node to find an adequate number of objects to blur its sensing area. When there are more objects, the sensor node finds smaller cloaked areas that satisfy the k-anonymity privacy requirement, as given in Fig. b. Thus, the required search space of a minimal cloaked area computed by the quality aware algorithm becomes smaller; hence, the communication cost of gathering the information of the peers in such a smaller required search space reduces. Likewise, since there are fewer peers in the smaller required search space as the number of objects increases, finding the minimal cloaked area incurs less MBR computation (Fig. c). Since our algorithms generate smaller cloaked areas when there are more users, the spatial histogram can gather more accurate aggregate locations to estimate the object distribution; therefore, the query answer error reduces (Fig. d). The result also shows that the quality-aware algorithm always provides better quality services than the resource-aware algorithm.



Fi Anonymity levels. (a) Communications cost. (b) Cloaked area size. (c) Computational cost. (d) Estimation error

CONCLUSION

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, which preserve personal location privacy, while enabling the system to provide allocation monitoring services. Both algorithms rely on this of 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>= 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, 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 provide location monitoring services through answering range queries. We evaluate our system through simulated experiments. The results show that our system provides high-quality lo-

cation monitoring services (the accuracy of the resource-aware algorithm is about 75 percent and the accuracy of the quality-aware algorithm is about 90 percent), while preserving the monitored object's location privacy.

REFERENCES

[1] C. Bettini, S. Mascots, X.S. Wang, and S.Jajodia, "Anonymity in Location-Based Services: Towards a General Framework," Proc.Int'l Conf. Mobile Data Management (MDM), 2007.

[2] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms," IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008.

[3] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIV_E: Anonymous Location-Based Queries in Distributed Mobile Systems," Proc. Int'l Conf. World Wide Web (WWW), 2007.

[4] H. Kido, Y. Yanagisawa, and T. Satoh, "An Anonymous Communication Technique Using Dummies for Location-Based Services," Proc. Int'l Conf. Pervasive Services (ICPS), 2005.

[5] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, "Privacy-Aware Location Sensor Networks," Proc. Ninth Conf. Hot Topics in Operating Systems (HotOS), 2003.

6] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The Anatomy of a Context-Aware Application," Proc. ACM Mob Co

[7] J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks," Proc.ACMMobiHoc,2003.