Survey On Location Anonymization Algorithms For Wsn

Giri M. S, Prof. Chirchi V. R

[1]*P.G. Department(CNE), MBES,COE Ambajogai ,M. S. India,*

[2]*IEEE Member P.G Department(CNE), MBES,COE Ambajogai ,M. S.India,*

Abstract

The advances in sensing and tracking technology enable location based many applications in wireless sensor network. These applications depends upon the information of personal locations. Monitoring personal locations with a potentially untrusted system poses privacy threats to the monitored individuals. The two algorithms are used , namely, resource-aware and quality-aware algorithms. Both algorithms established k-anonymity privacy concept to enable trusted sensor nodes to provide the aggregate location information .These algorithm aims to provide high quality location monitoring services for system users. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations. It use a spatial histogram approach that estimates the distribution of the monitored persons based on the gathered aggregate location information. It guarantees the location privacy of the monitored persons in wireless sensor network.

***Keywords*— *k*-anonymity, spatial histogram, privacy, aggregate Location, wireless sensor network**

1. Introduction

Wireless sensor networks (WSN) is a large collection of spatially distributed, autonomous devices or nodes that communicate through wireless and cooperatively monitor physical or environmental conditions. The sensor nodes such networks are deployed over a geographic area. Each sensor node can only detect events within a very limited distance, called the sensing range of the sensor node. Sensor nodes normally have fairly limited transmission and reception capabilities so that sensing data have to be passed through multi-hop path to a distant base station (BS), which is a data collection center with sufficiently powerful processing capabilities and resources.

Monitoring personal locations with a potentially untrusted system poses privacy threats to the monitored individuals. Privacy is an important concept in our society, and has become very vulnerable in these technologically advanced times. Many technology has been proposed to protect individual privacy; a key component is the protection of individually identifiable data. Monitoring personal locations with a potentially untrusted system poses privacy threats to the monitored individuals, because an adversary could abuse the location information gathered by the system. The concept of aggregate location information is a collection of location data relating to a group or category of persons from which individual identities have been removed. It proposes a privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services. The well established k-anonymity privacy concept requires each person is indistinguishable among k persons. A smaller k indicates less privacy protection, because a smaller cloaked area will be reported from the sensor node. However, a larger k results in a larger cloaked area will reduce the quality of monitoring services, but it provides better privacy protection. The system can avoid the privacy leakage by providing low quality location monitoring services for small.

It has 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 sensor areas into cloaked areas.

Most commonly used privacy enhancing technique is to blur the users exact location into spatial region that is spatial cloaking .Spatial cloaking means extending the possible user location to entire region.

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 . The quality - aware algorithm starts from a cloaked area, which is computed by the resource-aware algorithm.

IJERT

It propose a spatial histogram that analyzes gathered aggregate locations to estimate the distribution of the monitored persons in the system. The estimated distribution is used to answer aggregate queries.

The results show that the communication and computational cost of the resource-aware algorithm is lower than the quality-aware algorithm, while the quality-aware algorithm provides more accurate monitoring services than the resource-aware algorithm. The resource-aware algorithm is suitable for the system, where the wireless nodes have scarce communication and computational resources, while the quality-aware algorithm is favorable for the system, where accuracy is the most important factor in monitoring services.

1.1 K-anonymity principle

While anonymity is define as "being nameless" or "of unknown authorship"[4], information privacy researchers interpret it in a stronger sense.

According to Pfitzmann and Koehntopp, "anonymity is the state of being not identifiable within a set of subjects, the anonymity set"[5]. Inspired by Samarati and Sweeney [6], we consider a subject as k-anonymous with respect to location information, if and only if the location information presented is indistinguishable from the location information of at least k 1 other subjects.

Privacy preservation we have generally found that as long as location information is aggregated over a group of individuals, release does not violate privacy. *k*-anonymity provides a formal way of generalizing. This concept is user is *k* anonymous if and only if it is indistinguishable among at least k users in its identifying information . The key step in making location information in anonymous is to generalization. The K-anonymity principle is :a query is considered private, if the probability of identifying the querying user does not exceed 1/K, where K is a user-specified anonymity requirement.

K anonymity requirement is "each release of data must be such that every combination of values of quasi-identifiers can be indistinctly matched to at least k -1 individuals".

2. Location Anonymization Algorithms

It propose resource-aware and quality-aware anonymization algorithms in wireless sensor networks .In this algorithm concept of *k*-anonymity privacy requirement is used. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas[1].

2.1 The Resource-Aware Algorithm

It indicates that the sensor nodes can communicate directly with each other. This algorithm consists of three steps: broadcast step, cloaked area step, cloaked area step. Algorithm 1 outlines the resource-aware location anonymization algorithm.

Algorithm 1: Resource-aware location anonymizat-ion algorithm

function RESOURCEAWARE (Integer k, Sensor m, List R)

2: *PeerList* ⟵ { Ø }

// 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 ϵ R **then**

IJERT

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**

Step 1: The broadcast step:

It is to guarantee that each sensor node knows an adequate number of objects to compute a cloaked area. To reduce communication cost, this step relies on a heuristic that a sensor node only forwards its received messages to its neighbors when some of them have not yet found an adequate number of objects.

In this step, after each node m initializes an empty list PeerList, m sends a with its identity m.ID, sensing area m.Area, and the number of objects located in its sensing area m.count, to its neighbors. When m receives a message from a peer p, m stores the message in its PeerList. Whenever m finds an adequate number of objects, m sends a notification message to its neighbors. If m has not received the notification message, some neighbor has not found an adequate number of objects, therefore m forwards the received message to its neighbors.

Step 2: The cloaked area step:

It is that each node blurs its sensing area into a cloaked area that includes at least k-objects 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 node initializes in its PeerList. It includes at least k-objects and has an area as small as possible. Finally, m determines the cloaked area that is a minimum bounding rectangle (MBR) that covers the sensing area of the nodes, and the total number of objects. An

MBR is a rectangle with the minimum area that completely contains all desired regions.

Step 3: The validation step

It is to avoid reporting aggregate locations with a relationship

to server. Each node maintains a list to store the aggregate locations sent by other peers.

2.2 The Quality-Aware Algorithm

The Quality-aware algorithm initializes a variable current minimal cloaked area. When the algorithm terminates, the current minimal cloaked area contains the set of sensor nodes. This algorithm consists of three steps.

Step 1: The search space step

It is too costly for 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 based on the input initial solution. It is to compute the minimal cloaked area.

Step 2: The minimal cloaked area step

It takes a set of peers in search space, computes the minimal cloaked area for the sensor node. It propose two optimization

techniques to reduce computational cost. The first optimization technique is that need not to examine all the combinations of the peers. This optimization mainly reduces computational cost by reducing the number of computations among the peers. The second optimization technique has two properties:

a. Lattice structure:

It is used to generate the combinations of the sensor nodes. It generates the lattice structure from the lowest level based on a simple generation rule.

b. Monotonicity property:

This property propose two pruning conditions in the lattice structure. 1. If the combination gives the current minimal cloaked area, other combinations that contains at the higher levels of the lattice structure\should be pruned. 2. If a combination constitutes a cloaked area that is the same or larger than the current cloaked area, other combinations that contain at the higher levels of the lattice structure should be pruned.

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

IJERT

5: Add each peer located in S to C[1] as an item

6: Add m to each itemset in C[1] as the _rst item

7: **for** i = 1; i <= 4; i ++ **do**

8: **for** each itemset X = {a_1…..a_{i+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={x_1….x_{i+1}}, Y ={y_1…..y_{i+1}} in C[i]

Do

20: **if** $x_1 = y_1$,…. $x_i = y_i$ and x_{i+1} !=y_i+1 **then**

21: Add an itemset {x_1…. x_{i+1}, y_{i+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*

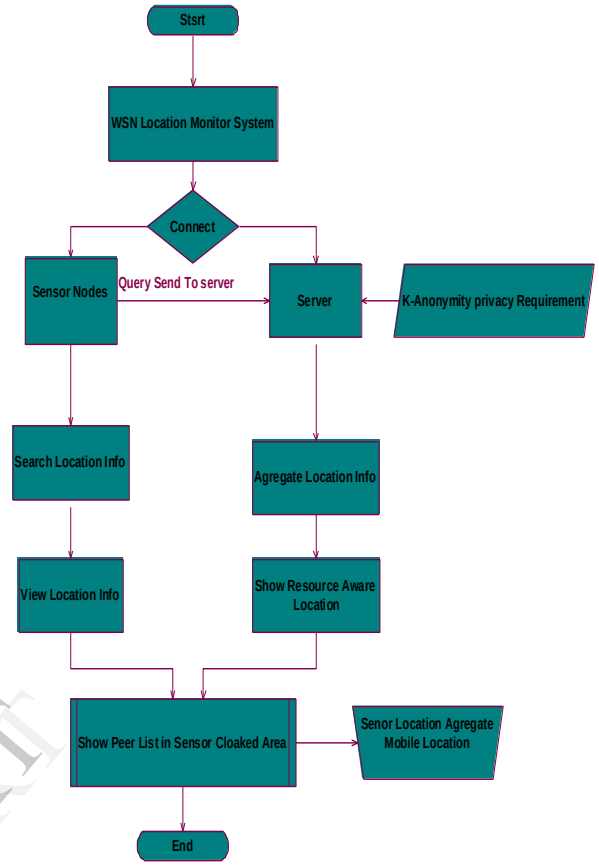
// Step 3: The validation step

28: Lines 18 to 25 in resource aware algorithm

4. Spatial Histogram

It use a spatial histogram which is embedded inside the server to estimate the distribution of the monitored objects based on the aggregate locations from the sensor nodes. The use of spatial histogram is to provide approximate location monitoring services. The accuracy of the spatial histogram that indicates the utility of location monitoring system will be evaluated [1].

3. Data flow diagram



IJERT

4. Spatial Histogram

It use a spatial histogram which is embedded inside the server to estimate the distribution of the monitored objects based on the aggregate locations from the sensor nodes. The use of spatial histogram is to provide approximate location monitoring services. The accuracy of the spatial histogram that indicates the utility of location monitoring system will be evaluated [1].

5. Conclusion

We study the location anonymization algorithm for wireless sensor networks. The two in-network location anonymization algorithms are resource-aware and quality-aware algorithms. These algorithm mainly uses the concept of k anonymity in which person is indistinguishable among k users. The resource-aware algorithm aims to reduce communication and computational cost while the Quality-aware algorithm aims to maximize the accuracy. The accuracy of Quality-aware algorithm which is 90% is higher when compared with resource-aware algorithm which is only 75%. It provides high quality location monitoring services.

6. References

[1] Chi-Yin Chow, *Student Member, IEEE,* Mohamed F. Mokbel, *Member, IEEE,* and Tian He, *Member,* "Privacy-Preserving Location Monitoring System for Wireless Sensor Networks " IEEE transactions on mobile computing, vol. 10, no. 1, jan 2011.

[2] Chi-Yin Chow, *Student Member, IEEE,* Mohamed F. Mokbel, *Member, IEEE,* and Tian He, *Member,* "Privacy-Preserving Location Monitoring System for Wireless Sensor Networks " IEEE transactions on mobile computing, vol. 10, no. 1, jan 2011.

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

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

[5] J.A. Simpson and E.S.C.Weiner, editors. Oxford English

Dictionary, Second Edition. Clarendon Press, 1989.

[6] Andreas Pfitzmann and Marit Koehntopp ." Anonymity,unobservability, and pseudonymity — a proposal for terminology". In Hannes Federrath, editor, Designing Privacy Enhancing Technologies — Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability, volume 2009 of LNCS. Springer, 2000.

[7] P. Samarati and L. Sweeney." Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression." Technical Report SRI-CSL-98-04, Computer Science Laboratory,SRIInternational,1998.

[8] Traf-SysInc,".People counting systems .http:// www .trafsys.com/products/peoplecounters/thermal-sensor.aspx.

[9] Bettini, S. Mascetti, X. S. Wang, and S. Jajodia, ."Anonymity in location-based services: Towards a general framework",. in *Proc.of MDM*,2007.

[10] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan,.Query
privacy in wireless sensor networks,. in *Proc. of SECON*, 2007.

[11] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan,.Private queries in location based services: Anonymizers are not necessary,.in *Proc.of SIGMOD*,2008.

IJERT