Implementation Of Location Monitoring Services Based On Anonymization Algorithm

J.Kartheeswari
Centre For Information Technology And Engineering, M S University, Tirunelveli

ABSTRACT

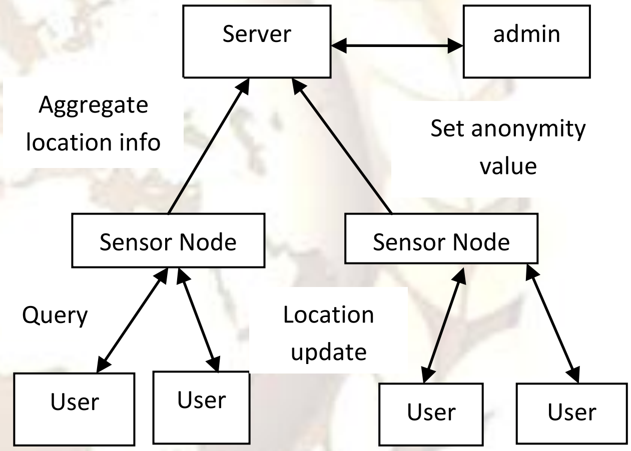
Anonymization algorithm is mainly used to monitor the location . In this paper propose an implementation of location monitoring services based on resource and quality aware algorithm. In resource aware algorithm to minimize time and communication cost. In existing system to find the minimum bounding rectangle using monitor area. In our paper another way to find the minimum bounding rectangle using monitor object. While finding the minimum founding rectangle with monitor object and monitor area we find that the time to process is equal.

Keywords – ***Wireless sensor networks, Location privacy, Aggregate location***

I. INTRODUCTION

In wireless sensor network (WSN) is an ad-hoc network composed of small sensor nodes deployed in large numbers to sense the physical world. Wireless sensor networks have very broad application prospects including both military and civilian usage. In mobile sensor network development of algorithms and prototype vehicles for wide-area surveillance and reconnaissance using mobile sensor networks (MWSN). Monitoring on land, water and air using large numbers of mobile sensor nodes is demonstrated at our Distributed Intelligence and Autonomy Lab (DIAL). Mobile sensor networks are sensor networks in which nodes can move under their own control or under the control of the environment. Mobile networked systems combine the most advanced concepts in perception, communication, and control to create computational systems capable of interacting in meaningful ways with the physical environment, thus extending the individual capabilities of each network component and network user to encompass a much wider area and range of data. A key difference between a mobile sensor network and a static sensor network is how information is distributed over the network. Under static nodes, a new task or data can be flooded across the network in a very predictable way. Under mobility this kind of flooding is more complex. Under natural mobility this depends on the mobility model of the nodes in the system. For the location monitoring system using identity sensors and counting sensors. In identity sensor location monitoring system, the sensor nodes report the exact location information of the monitored persons to the server. While counting sensor monitoring system, each sensor node reports the number of objects in its sensing area to the server. We propose two anonymization algorithm namely Resource-aware and Quality-aware algorithm. In Resource aware algorithm to minimize communication cost. In quality aware algorithm to provide accurate location.

II. SYSTEM ARCHITECTURE



Sensor Nodes: Each sensor node is responsible for determining the number of objects in its sensing area. Sensor nodes blurs its sensing area into a cloaked area, which includes at least k objects, and reports with the number of objects located in particular region as an aggregate location information to the server. Each sensor node is also aware of its location and sensing area.

Server: Server collects the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects. Also server answers range queries raised by users, based on the estimated object distribution. 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.

Users: Each and every user updates their location information to the sensor node. Users can issue range queries to the system through the sensor nodes. They can get reply for query like, what is the number of persons in a certain area? The server uses the spatial histogram to answer their queries.

Privacy model: Sensor nodes constitute a trusted zone, communicate with each other through a secure network channel to avoid internal network attacks, for example, eavesdropping, traffic analysis, and malicious nodes. The system 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. Authenticated administrators can change the k-anonymity level. 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 the algorithm to get the original readings from the sensor nodes, in order to get the best services from the system. This is a nice 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 anonymized level gets stricter.

Aggregate Location: Each sensor node blurs its sensing area into a cloaked area, in which at least k persons are residing. Each sensor node reports only aggregate location information, which is in a form of a cloaked area A, along with the number of persons, N, located in A, where N ≥ k, to the server. A smaller k indicates less privacy protection, because a smaller cloaked area will be reported from the sensor node; hence better monitoring services. A larger k results in a larger cloaked area, which will reduce the quality of monitoring services, but it provides better privacy protection.

III. RESOURCE AWARE ALGORITHM

Resource aware algorithm indicates that the sensor nodes can communicate directly with each other. This algorithm consists of three steps.

3.1 Broadcast Step

Broadcast step 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 sensor 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 neighbors has not found an adequate number of objects, therefore m forwards the received message to its neighbors.

3.2 Cloaked Area Step

Cloaked area step is that each sensor node blurs its sensing area into a cloaked area that includes alteast 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.

3.2.1 Score

The score is defined as a ratio of the object count of the peer to the euclidean distance between the peer and m. The idea behind the score is 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

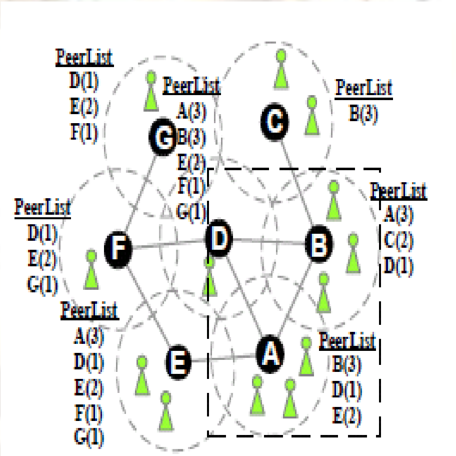


Figure 2. Resource aware cloaked area of sensor A

Figure 2. illustrates the cloaked area step. The PeerList of sensor node A contains the information of three peers, B, D, and E. The object count of sensor nodes B, D, and E is 3, 1, and 2, respectively. We assume that the distance from sensor node A to sensor nodes B, D, and E is 17, 18, and 16, respectively. The score of B, D, and E is 3/17 = 0:18,1/18 =0:06, and 2/16 = 0:13, respectively. Since B has the highest score, we select B. The sum of the object counts of A and B is six which is larger than the required anonymity level k = 5, so we return the MBR of the sensing area of the sensor nodes in S, i.e., A and B, as the resource-aware cloaked area of A, which is represented by a dotted rectangle.

3.2.2 Minimum Bounding Rectangle

For each sensor node initializes in its PeerList. It includes atleast 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.

3.3 Validation Step

In validation step is to avoid reporting aggregate locations with a relationship to server Each sensor node maintains a list to store the aggregate locations sent by other peers. AS this step ensures that no aggregate location with the containment relationship is reported to the server, the adversary cannot obtain any deterministic information from the aggregate locations. Since the server receives an aggregate location from each sensor node for every reporting period, it cannot tell whether any containment relationship takes place among the actual aggregate locations of the sensor nodes.

IV 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.

4.1 Search Space Step

The search space step 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.

4.2 Minimal Cloaked Area Step

Minimal cloaked area 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

1. Lattice Structure
2. Monotonicity Property

4.2.1 Lattice structure:

Lattice structure 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. In lattice structure concept used for to finding the minimum bounding rectangle. In existing system to find the minimum bounding rectangle using monitor area. In our paper another way to find the minimum bounding rectangle using monitor object.

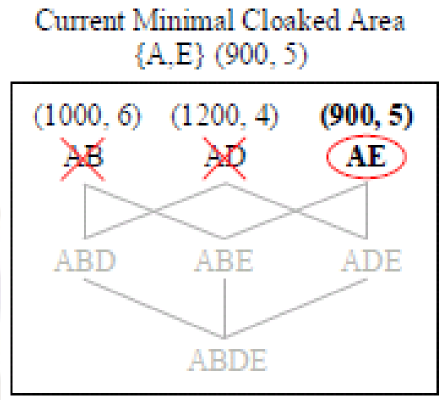


Figure 3. Quality aware cloaked area of sensor A

Figure 3 illustrate the area of MBR $\{A,E\}$ is less than current minimal cloaked area and the total number of monitored objects in MBR $\{A,E\}$ is k= 5, we set $\{A,E\}$to the current minimal cloaked area

4.2.1 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 minimal cloaked area, other combinations that contain at the higher levels of the lattice structure should be pruned.

4.3 Validation Step

This step is exactly the same as in the resource-aware algorithm.

V IMPLEMENTATION

In this application, we try to implement location monitoring system. We use MS access as database for this application. We are going to develop a location monitoring system, where user updates their location to server through sensor node. Sensor node cloaks the exact location of client to region coverage range, thus the privacy of the user can be preserved. Also more privacy can be achieved by using k-anonymity value, which can be set by admin. More the value of k-anonymity means more privacy for users. The users in particular region can rise query to server about the number of users in that particular region. In our system, the sensor nodes constitute a trusted zone, and communicate with each other through a secure network channel to avoid internal network attacks, for example, eavesdropping, traffic analysis, and malicious nodes.

The aggregate location using k-anonymity value can arrived in the coming phase. Also the coming phase work includes, the given 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. 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.

We Well established k-anonymity privacy, that is, a person is indistinguishable among k persons. Enables trusted sensor nodes and provides the aggregate location information of monitored persons .Each aggregate location is in a form of a monitored area A along with the number of monitored persons residing in A, where A contains at least k persons. The resource-aware algorithm aims to minimize communication and computational cost .Quality-aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas. While finding the minimum bounding rectangle with monitor object and monitor area we find that the time to process is equal.

CONCLUSION

In this paper we propose implementation of location monitoring services based on anonymization algorithm. 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. While finding the minimum bounding rectangle with monitor object and monitor area we find that time to process is equal.

REFERENCES

[1] D. Culler and M.S. Deborah Estrin, "Overview of Sensor Networks," Computer, vol. 37, no. 8, pp. 41-49, Aug. 2004.

[2] Kido, H.;Yanagisawa,Y.; Satoh, T. " An anonymous communication technique using dummies for location-based services Pervasive Services" ICPS '05. Proceedings. International Conference on Publication ,pp: 88 – 97,2005

[3] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge and Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.

[4] C.-Y. Chow, M.F. Mokbel, and X. Liu, "A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-Based Services," Proc. 14th Ann. ACM Int'l Symp. Advances in Geographic Information Systems (GIS), 2006.

[5] Jiejun Kong , Xiaoyan Hong, ANODR: *anonymous on demand routing with untraceable routes for mobile ad-hoc networks*,2005

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

[7] 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.

[8] T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-Based Services," Proc. IEEE INFOCOM, 2008.

[9] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD, 2008.

[10] S. Guo, T. He, M.F. Mokbel, J.A. Stankovic, and T.F. Abdelzaher, "On Accurate and Efficient Statistical Counting in Sensor-Based Surveillance Systems," Proc. Fifth IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS), 2008.

[11] K. Bohrer, S. Levy, X. Liu, and E. Schonberg, "Individualized Privacy Policy Based Access Control," Proc. Sixth Int'l Conf. Electronic Commerce Research (ICECR), 2003.

[12] E. Snekkenes, "Concepts for Personal Location Privacy Policies," Proc. Third ACM Conf. Electronic Commerce (EC), 2001.

[13] L. Sweeney, "Achieving k-Anonymity Privacy Protection Using Generalization and Suppression," Int'l J. Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 571-588, 2002.

[14] 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.

[15] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," Proc. Int'l Conf. World Wide Web (WWW), 2008.