Location Monitoring and Privacy Preserving in WSN

Abstract—Wireless sensor network are spreading their wings extensively from military and surveillance application to many other fields. Generally it is seen that such systems if have an untrusted server implies many security problems within the system especially for the monitored entities. These problems would be an revealed hidden identity or problems like misusing of personal location sensitive information of the monitored entity. Mainly WSN systems have two main components which are the driveway to the system, they are sensor nodes and descendant node. Sensor nodes detect the environmental or physical conditions in its coverage area and pass it ahead for further processing. Descendant or the last final node collects all the information and collectively from every other node and sends it to the server where it is stored and further processed. Any system which provides monitoring services should be secure enough that personal sensible data should be protected by it for the system hygiene. Thus monitoring services with high-end quality should be given by any system along with protecting the privacy of the monitored being is a must for the system to achieve balance in between with. A well thought of way which recent systems use is to restrict the sensor nodes from sending information about individual entities and rather make them report aggregate location information regarding monitored individuals. This maintains the privacy aspect for the system. The proposed system taking all these things in consideration makes use of two location-anonymization algorithms which in turn makes use of k-anonymity concept. The two algorithms used are Resource-aware and Quality-aware algorithms respectively. Both of them work on the k-anonymity concept. Using these modules in the proposed system, any sensor node is restricted to send an aggregate location information to the server which at least has k monitored beings in its area; if less then it waits till the number in its area becomes minimum ‘k’ and then sends the information further. Thus the system in this way as its name suggests preserves the privacy as well as provides excellent monitoring services for its users. Based on this information the server plots a spatial histogram through which it answers the range queries fired by the end users of the system. Thus k-anonymity concept in its base-line notifies that though reporting is done on an aggregate basis still every monitored being is un-identifiable among k different beings. The evaluation of the proposed system is don’t through many different inputs and observations. The final output which is produced by the system notifies that the system successfully and qualitatively monitors the entities in its area and yet preserves their privacy aspect by reporting their overall aggregate location information.

Keywords—Monitored beings, Wireless Sensor Network, k-anonymity, Resource-aware, Quality-aware, Spatial Histogram, Server.

I. INTRODUCTION

Location monitoring systems have found scope more in recent years for civilian purposes. Besides wireless Sensor networks is collection of few base stations and hundreds or less sensor nodes which are deployed randomly. [1] These sensors are used to detect physical such as movements and position and environmental conditions such as temperature, humidity etc. For the same they generally make use of either Identity sensors or Counting sensors. Both of these provide monitoring for location-dependant situations. Identity sensors have individually carrying a signal sending-receiving element with it with allotted a unique Identification associated with it. This ID is a globally unique ID. Thus identity sensors have the ability to locate the exact location of the monitored being. This can turn harmful as if the server or end users are unauthorised or untrusted, this personal insightful data can be misused by them. Counting sensors on the other hand report the no. of monitored beings in their area instead of a single entity. This may also pose problems though indirectly for the system. E.g. In a hospital where counting sensors are deployed and a third person untrusted of course, if want to extract the systems personal information he can do it. Suppose there are only few entities are present at time t1 to be monitored and some of them are fixedly placed in their location areas then the remaining entities information can be calculated based on their movements throughout the system like rooms/departments they visit, health records and no. of times the entity visited certain clinical rooms, etc. In short, both the situations may prove dangerous for the system and its monitored beings thus a balance between the two needs to be achieved. The optimal solution for the above problem is to hide individual information yet reporting aggregate location information to the server. The projected system serves this purpose by using two well-known location anonymization algorithms namely Resource-aware and Quality-aware algorithms. Both these algorithms make use of k-anonymity concept which states that each monitored entity is indistinguishable among ‘k’ different persons.
Resource-aware algorithm takes input a set of enough individuals to be monitored, and processes it to form a cloaked area of it. Quality-aware take input as the cloaked area and refines it iteratively to form a minimal-sized cloaked area. Sensor nodes for both of these algorithms report this cloaked area ‘A’ along with no. of monitored entities in it to the server. Server on the basis of this information further plots a spatial histogram which depicts the distribution of these monitored entities across cloaked areas. Whenever the end users of the system fire range queries such as how many beings are there in area A1? etc. and many more like this, are all answered by the server. Thus path from the sensor nodes and the server is made secure by reporting aggregate location information to the server and server to the end users is also secured by answering only range queries and applying this k-anonymity concept.

II. EXISTING SYSTEM

Most of the existing systems have preferred use of counting sensors rather than identity sensors for their location monitoring services. Sensors have played a very important role in the whole process of locating and monitoring entities. Sensor nodes are deployed such that they detect and locate the entities in their sensing areas. The entire process basically works like this:

A. Sensing of sensor nodes

Sensor nodes (either Counting or Identity sensors) are used to locate and detect location information of entities being monitored in their areas. Each sensor node is responsible for estimating the no. of entities in its area. They sense the location information around for monitored beings and send it to the server i.e. they report it to the server for further processing.

B. Passing data to server

Server after receiving the data from all the sensor nodes analyses it and starts further processing. It plots a spatial histogram based on the information received from all the nodes and thus depicts the distribution of monitored beings across all sensing areas.

C. Server serving end users

Server is ultimately responsible for serving the end-users of the system. End users query the server for the location related information and server answers their queries looking at this spatial histogram plotted by it. Thus spatial histogram estimates the distribution of monitored objects throughout the system’s sensing areas.

III. PROPOSED SYSTEM

The proposed system works keeping in mind the existing system features and add some extra feature of its own thus making it more powerful and complete in its own sense. The proposed system works on the following elements. These elements together work collaboratively towards the execution of the systems function as a whole. Thus the elements of the system are described below:

A. Sensors

Sensor nodes are solely responsible for sensing objects in their respective coverage areas. After sensing these objects, they are reported as no. of objects in area ‘A’ along with the Id of area A and sensor ID by the respective sensor to the server. Server comes to know how many objects are there in a area, who is the sensor responsible for reporting this information and which area the sensor belongs to from the report of the sensor side. Each sensor node knows its sensing area ‘A’ and its location information. Sensor nodes are limited by a well-known k-anonymity concept implemented within the system which allows sensor nodes to report no. of nodes in its area only when it has enough no. of objects in its area i.e. objects at least equal to ‘k’ or more than that; but the objects should not be less in no. than ‘k’.

B. K-anonymity concept

As mentioned earlier, sensor nodes work on the k-anonymity concept. It means that every individual entity is indistinguishable from all other ‘k’ entities and that any sensor node can report to the server only when it has got enough number of objects in its area i.e at least equal to or more than ‘k’. Thus sensor nodes cannot report the objects in their areas till they are less in number than ‘k’.
Thus k-anonymity concept sees to it that the sensor nodes can report thus aggregate location information to the server. No. of objects in the area ‘A’, Area ID and sensor ID are the three things reported by the sensor node to the server.

C. Resource-aware algorithm

Data from the sensor nodes goes for intermediate processing through Resource aware algorithm first. This algorithm accepts input from the sensor nodes i.e. set of monitored beings in an area and forms a cloaked area based on this information. This cloaked area satisfies the k-anonymity based on this information. This cloaked area satisfies the k-anonymity concept.

D. Quality-aware algorithm

As resource-aware takes input as set of objects in a particular area and forms a cloaked area out of it; this cloaked area is given as input to quality-aware algorithm. Thus this algorithm accepts input as a cloaked area; it refines it iteratively to form a minimal-sized cloaked area out of it.

E. Server module

Server is ultimately responsible to for two main functions namely: To design/plot the spatial histogram and answer the end-user queries based on the readings of this spatial histogram. Minimal formed cloaked area is submitted to the server module which plots the spatial histogram from the inputs it receives from the sensor nodes. After plotting the histogram, end-user range queries are fired to the system which server answers. He answers them by observing the readings of the spatial histogram.

F. Spatial histogram

Spatial histogram is plotted to calculate the distribution of monitored objects. It is plotted on the basis of the information reported by various sensor nodes regarding the no. of nodes in their area, their Area ID and sensor ID. The purpose of a spatial histogram is to provide accurate location monitoring services. It is nothing but a two-dimensional array of m rows and n columns which depict the distribution of monitored objects across different sensing areas.

G. End-user queries

End users fire range queries on the system which server answers solely. Server module answers the range queries like how many objects are there in area ‘A’? etc.

IV. ALGORITHMS USED

A. Resource-aware algorithm

The resource-aware takes input as a set of monitored objects and give output as a cloaked area formed out of it. It works in the following manner as shown below

//Broadcast stage

Step1: Each sensor node will send a message containing its own ID, its area ID and no. of objects in its area to its neighbor peers.

Step2: If a sensor node gets a message as in step 1, it will add that message to its peer list.

Step3: If adequate no. of objects in its peer list, sensor node will send an alert message to its neighbor sensors else it will continue forwarding those messages to its neighbor sensors till it is needful to do so.

//Cloaked area stage

Step4: Estimates score for every peer in the peer list of each sensor node.

Step5: continue selecting the peer with highest score from the peer list and adding it to S where S is the minimum surrounding area of a sensor node and N is the number of objects in S.

//Validation stage

Step6: If there is no common area or containment relationship between sensor nodes then no reporting of the aggregate location to the server else aggregate location information is reported to the server by the sensor node.

B. Quality-aware algorithm

Quality-aware algorithm accepts the cloaked area as input and gives output a minimal formed cloaked area. It works in the following manner as shown below:

//Search-space stage

Step1: Assume a Search area S depending on the initial solution.

Step2: Estimate the information of all the peers located in that area.

//Minimum cloaked area stage

Step3: Compute the minimal cloaked area for a set of peers included in ‘S’ by searching for any 4 combinations of peers.
(NOTE: MBR (Minimum Bounded Rectangle) requires at the most 4 sensor nodes to define itself out of which two define the breadth of the sensor node parallel to the x-axis and other two define the tallness of the sensor node parallel to y-axis).

//Validation stage

Step4: Check for the containment relationships (if any). If no such relationships, then report the aggregate location to the sever.

NOTE: This step is exactly similar to the validation stage of Resource-aware algorithm.

V. Final Results
As in our proposed system and the overall working of the two algorithms, we can say that cloaked area processing is done by both the algorithms. But resource-aware makes a general cloaked area and quality-aware makes a refined minimal cloaked area out of the information they get. Fig. 2. Shows the approximate size that exact algorithm will be making the cloaked area of. Since a refined minimal cloaked area is iteratively refined again and again till it reaches the desired minimum size, the size of the cloaked area formed in quality-aware algorithm will be comparatively smaller than in resource-aware algorithm. 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 is. Thus we can measure the Clocked Area Collected and processed with the help of both Quality Aware and Resource Aware Algorithm. Fig. 3. Shows a crucial comparison between resource-aware algorithm and quality-aware algorithm with respect to communicational 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. Thus providing comparison mechanism for the evaluating communication cost required by the resource aware and Quality aware algorithm. Fig. 4. Shows we measure the computational cost of our location anonymization algorithms 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 Resource aware Approach MBR for each combination of the peers in the required search space to find the minimal cloaked area. The Resource aware approach does not employ any optimization techniques proposed for our quality-aware algorithm thus providing effective MBR computation comparisons for cost of the computation. [2] In general the resource-aware reduces the computational and communicational cost whereas the quality-aware reduces the cloaked area size for the system.

VI. COMPARISON BETWEEN EXISTING SYSTEMS AND PROPOSED SYSTEM

Many existing systems earlier have used different anonymization techniques for securing the basic property for their system. Existing systems however felt the real need to protect the location information for the monitored objects of their respective systems and thus implemented many different techniques to prevent these sensitive data from untrusted server or unauthorized users. One of those techniques was false locations which were used in earlier systems. It means while reporting any one location for a object, the sensor nodes used to report ‘n’ different locations for the same object out of which only one location was the true location of the object and others were termed as false locations. This increased the piling up of false data (too many) at the servers end causing a lot many data duplication problems. Spatial cloaking was another technique which was used in which blurring the area of the monitored object, thus satisfying the privacy requirement of the system. Our proposed system makes use of spatial cloaking technique as it provides aggregate location information to the server and thus preserves the privacy requirement of the system through k-anonymity concept and minimal cloaked area scheme. In addition our system keeps in mind that only the sensor nodes are internal to the system and threats occurring to the system may arrive from the server side as it can be untrusted or user side as they are external to the system. Thus many security mechanisms are implemented on both the sides so as to secure the system from external aspects. Only the administrator has right to decide on the value of ‘k’ for the system and he is the one who can change the value. Besides this, only authorized users are allowed to query the system. This authorization ifs provided by valid user accounts created by the system administrator and managing them so as needed. Along with these measures we also have kept in mind that though all sensor nodes communicate with each other through a secure communication way, still the server to and server to end-user communication path as well needs to be protected. Thus RSA technique monitors the whole communication path from sensor nodes to servers as well as server module to the end-users. RSA is basically an asymmetric encryption system which is used to encrypt and decrypt messages; this entirely is done through keys namely public key and private keys. Thus every node generates these keys but public key is distributed or known to every one and private key is not known to everyone. In other words in general RSA technique, any one of the keys either public or private can be used to encrypt the message while the opposite/alternate key for encryption is used to decrypt the message. RSA technique is also called as public Key cryptography technique.

VII. CONCLUSION

Our proposed system thus achieves a balance between high-quality location monitoring services and thus as well yet preserving the privacy of those monitored objects through a k-anonymity concept. It performs this by two algorithms namely resource-aware and quality-aware algorithm respectively.
Resource-aware algorithm accepts the no. Of monitored objects and forms a so to say roughly estimated-sized cloaked area. This cloaked area is refined iteratively again and again to form a minimal formed cloaked area. This cloaked area is reported to the server which plots a spatial (two-dimensional) histogram based on the information it receives from the sensor nodes. Observing this spatial histogram the server module answers all the range queries fired by the end-users to the system. The entire communication path within and outside the system entities is governed by RSA technique.

REFERENCES


