Improving Source Location Privacy and Network Life Time in Energy Efficient Manner

M. Oviya
Final year student Department of Computer Science Engineering, E.G.S.Pillay Engineering College Nagapattinam

G. Nithiyabharathi
Final year student Department of Computer Science and Engineering, E.G.S.Pillay Engineering College, Nagapattinam

K. Balasubramanian
Assistant professor
Department Of Computer Science Engineering, E.G.S.Pillay Engineering College Nagapattinam

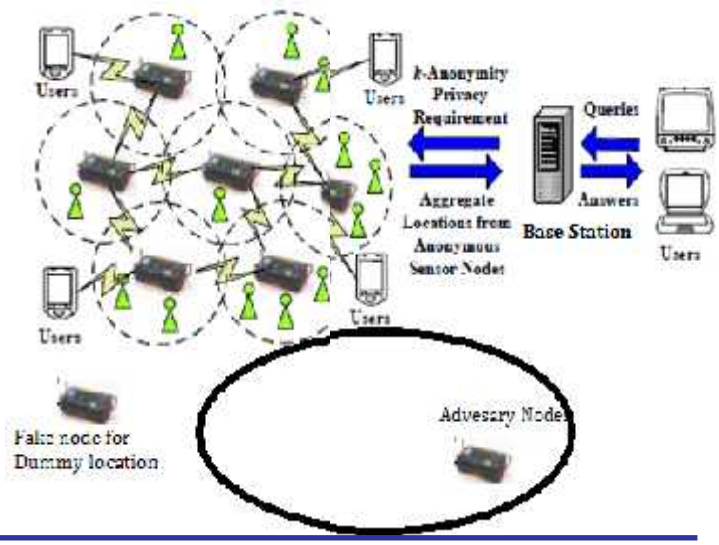
***Abstract*— monitoring personal locations with a potentially untrusted server poses privacy threats to the monitored individuals. It is proposed that a privacy-preserving location monitoring system for wireless sensor networks. It is designed that two WSN networks with fake source nodes support for every sender, to enable trusted sensor nodes to provide the aggregate location information of monitored persons (base Station) for our system. Every aggregate location is in a form of a monitored area A along with the number of monitored persons reside in A, where A hold at least k persons. To utilize the aggregate location information to provide location monitoring services, it is used that a structural histogram approach that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then the predicted distribution is used to provide location monitoring services through answering range queries. It is figure out that through simulated experiments. The results display provides high quality location monitoring services for system users and guarantees the location privacy of the monitored**

I. INTRODUCTION

The advance in wireless sensor technologies has resulted in many new applications for military and/or civilian purposes. Many cases of these applications expect on the information of personal locations, surveillance and location systems. These location-dependent systems are accomplished by using either identity sensors or counting sensors. For identity sensors, for Bat and Cricket, every individual has to carry a signal sender/receiver unit with a globally unique identifier. With identification sensors, the system can pinpoint the exact location of each monitored person. On the other hand, counting sensors, example, photoelectric sensors, and thermal sensors, are distribute to report the number of persons located in their sensing areas to a server.

Unfortunately, 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 to infer personal sensitive information. For 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. To tackle such a privacy breach, the concept of aggregate location information, that is, a collection of location data relating to a group or category of persons from which individual identities have been removed, has been suggested as an effective approach to preserve location privacy. Although the counting sensors by nature provide aggregate location information, they would also pose privacy breaches.

It is proposed that a privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services. It is released that on the well established k-anonymity privacy concept, which requires each person is indistinguishable among k persons. 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, to preserve personal location privacy; it is proposed that 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 sensing areas into cloaked areas, such that each cloaked area contains at least k persons to constitute a k-anonymous cloaked area. 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 reported to the server. In the resource-aware algorithm, each sensor node finds an adequate number of persons, and then it uses a greedy approach to find a cloaked area. On the other hand, the quality-aware algorithm starts from a cloaked area A, which is computed by the 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.



It is evaluated that through simulated experiments. 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 (the average accuracy is about 90%) than the resource-aware algorithm (the average accuracy is about 75%). Both algorithms only reveal k-anonymous aggregate location information to the server, but they are suitable for different system settings. The resource-aware algorithm is suitable for the system, where the sensor 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.

II. PROBLEM DEFINITION:

This work is not applicable to some landscape environments, for example, shopping mall and stadium, and outdoor environments. Our work distinguishes itself from this work, as it does not assume any hierarchical structures, so it can be applied to all kinds of environments. It is considered the problem of how to utilize the anonymized location data to provide privacy-preserving location monitoring services while the usability of anonymized location data was not discussed in other privacy related works include: anonymous communication that provides anonymous routing between the sender and the receiver.

PROCESS FLOW DIAGRAMS FOR EXISTING AND PROPOSED SYSTEM:

FEASIBILITY STUDY:

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

I. ECONOMICAL FEASIBILITY
II. TECHNICAL FEASIBILITY
III. SOCIAL FEASIBILITY

IECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

II.TECHNICAL FEASIBILITY:

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

III.SOCIAL FEASIBILITY:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

A. FUNCTIONAL REQUIREMENTS:

Functional requirements specify which output file should be produced from the given file they describe the relationship between the input and output of the system, for each functional requirement a detailed description of all data inputs and their source and the range of valid inputs must be specified.

B. NON FUNCTIONAL REQUIREMENTS:

Describe user-visible aspects of the system that are not directly related with the functional behavior of the system. Non-Functional requirements include quantitative constraints, such as response time (i.e. how fast the system reacts to user commands.) or accuracy ((.e. how precise are the systems numerical answers.)

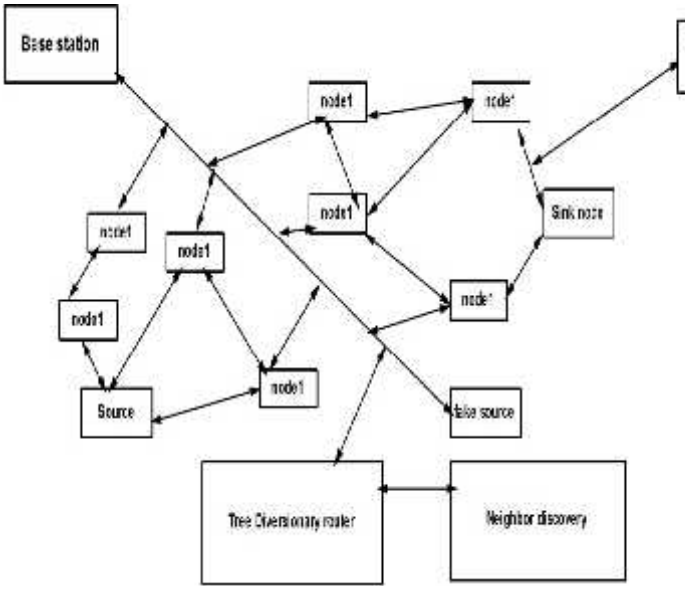
C. PSEUDO REQUIREMENTS:

The client that restricts the implementation of the system imposes these requirements. Typical pseudo requirements are the implementation language and the platform on which the system is to be implemented. These have usually no direct effect on the user's view of the system.

III. MODULES DESCRIPTION:

1. Backbone Route Path Establishment:

The previous section has given the number of branches through the analysis of relationship between energy consumption and network lifetime.It is discussed that the location of the backbone route to achieve security. With phantom route strategy, there is only one route path, which is the shortest path from phantom node to the sink, so the route path depends on the phantom node. Most researchers think that phantom node should be selected randomly, and further studies propose that the route path should avoid visible area.



2. Designing Tree Based Diversionary Routing:

Based on the network model discussed above, tree based route scheme includes three stages: (1) Tree-based diversionary routing establishment; (2) Stable operation stage of the tree-based routing; and (3) Destruction of tree-based diversionary routing. It is worth noting that it is adopted that the same method of creating a phantom node from. The requirement of choosing a phantom node is that the phantom node is as far away from the source node. In the following, it is described that the proposed tree-based diversionary routing in details.

3. Improving Network Lifetime:

In many existing studies, the privacy and energy consumption are contradictory. More diversionary routes require extra energy consumption, thus affecting the network lifetime. Generally, after the first nodal death, the network cannot completely and effectively monitor the monitoring area. Therefore, the network lifetime is usually defined as the first node death time. Obviously, to maximize the network lifetime, the key is to reduce the energy consumption in hotspot. Therefore, it is minimized that the energy consumption in the hotspots and at the same time. Establish diversionary routes by fully using of abundant energy in non-hotspot regions in order to improve the network lifetime.

4. Privacy Management:

In phantom routes, data of phantom node is sent to the sink according to the shortest routing protocol, therefore the adversaries can trace back to the phantom node. Previous studies have shown that, adversaries can still trace to the source node with a relatively high possibility. Therefore, one possible solution is to make it difficult for adversaries to trace to the phantom node, so that will be impossible to trace the source node. The proposed scheme first establishes a backbone route direct to the network border with diversionary routes as its branches. Then, it establishes diversionary routes as many as possible with each diversionary route directing to the network border, forming a tree based routing path. The data packet length and the data generating possibility are the same in each diversionary route.

IV ALGORITHM:

Tree Based Routing Algorithm - To find routing path based on trees

Algorithm implementation resides to get reliable path based on available tree view. The routing process will be done at before transmission for every hop or single hop mode. The data receiver may be transmitter or receiver.

Steps

1.) Discover your neighbors and learn their addresses.
2.) Measure the cost (delay) to each neighbor.
3.) Construct a packet containing all this information
4.) Send this packet to all other routers.
5.) Compute the shortest path to every other router.

Widely used today, replaced Distance Vector in the ARPANET. Link State improves the convergence of Distance Vector by having everybody share their idea of the state of the net with everybody else (more information is available to nodes, so better routing tables can be constructed).

The basic outline is

1. discover your neighbors
2. measure delay to your neighbors
3. bundle all the information about your neighbors together

Send this information to all other routers in the subnet

Compute the shortest path to every router with the information you receive.

Details:

1. Neighbor discovery

Send a packet out. Receiving routers respond with their addresses, which must be globally unique.

2. Measure delay

Time the round-trip for an ECHO packet, divide by two. Question arises: do you include time spent waiting in the router (i.e. load factor of the router) when measuring round-trip ECHO packet time or not?

3. Bundle your info

Put information for all your neighbors together, along with your own id, a sequence number and an age (flooding)

4. Distribute your info

Ideally, every router would get every other router data simultaneously. This can't happen, so in effect you have different parts of the subnet with different ideas of the topology of the net at the same time. Changes ripple through the system, but routers that are widely spread can be using very different routing tables at the same time. This could result in loops, unreachable hosts, and other types of problems.

A flooding algorithm is used to get the data out as soon as possible. The sequence number is used to control the flooding. Each router keeps track of the routing data packets it has seen by router/sequence number pair. If the pair is new, then it is forwarded on all lines but the one it arrived on, if it has been seen before it is not forwarded.

The age of a data packet is used to prevent corruption of the sequence number from causing valid data to be ignored. The age field is decremented once per second by the routers which

forward the packet. When it hits zero it is discarded.

How often to exchange data?

Compute shortest path tree - Using an algorithm like Dijkstra's, and with a complete set of information packets from other routers, every router can locally compute a shortest path to every other router. The memory to store the data is proportional to k * n, for n routers each with k neighbors. Time to compute can also be large. Bad data (from routers in error, e.g.) will corrupt the computation. When a neighbor sends you its routing table you examine it as follows and update your own routing table.
Pseudo Code:

```
For (i varied across all routers in the table)
{
   if (your distance to the neighbor + neighbors distance to router i  <  your previous estimate to router i )
{
      Your distance to router i = your distance to the neighbor + neighbors distance to router i

      Link to router i is set to link to the neighbor with the short distance to i
   }
}
```

Back bone route path creation :
Network life is retained when the exiting path is getting failure. This enhance the life time of the routing path

Backbone Implementation (Central routing of Network):
The backbone is the first area you should always build in any network using (open shortest path) OSPF and the backbone is always Area 0 (zero). All areas are connected directly to the OSPF backbone area. When designing an OSPF backbone area, you should make sure there is little or no possibility of the backbone area being split into two or more parts by a router or link failure. If the OSPF backbone is split due to hardware failures or access lists, sizeable areas of the network will become unreachable. This is the place where many fake sources are viewing itself as real source. These kind of nodes as fetched when adversary searched the message's sender.
TECHNIQUES AND ALGORITHM USED:
ALGORITHM:

1. *THE RESOURCE-AWARE ALGORITHM:*

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, it is proposed 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. It is evaluated that through simulated experiments.

V.CONCLUSION:

It is proposed that a privacy-preserving location monitoring system for wireless sensor networks. It is designed that 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 _ 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, it is proposed that 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. It is evaluated that through simulated experiments.

Good Teachers are worth more than thousand books, we have them in Our Department.

REFERENCE

[1] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, .Theanatomy of a context-aware application,. in*Proc. of MobiCom*,1999.

[2] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar,.SPINS: Security protocols for sensor netowrks,.in*Proc. of MobiCom*,2001.

[3] B. Son, S. Shin, J. Kim, and Y. Her, .Implementation of the realtimepeople counting system using wireless sensor networks,.*IJMUE*, vol. 2, no. 2, pp. 63.80, 2007.

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

[5] J. Kong and X. Hong, .ANODR: Anonymous on demand routingwith untraceable routes for mobile adhoc networks,.in*Proc. OfMobiHoc*, 2003.

[6] .Location Privacy Protection Act of 2001, http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp..

[7] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald,.Privacy-aware location sensor networks,. in*Proc. of HotOS*, 2003.

[8] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, .Thecricket location-support system,.in*Proc. of MobiCom*, 2000.

[9] Onesystems Technologies, .Counting people in buildings.http://www.onesystemstech.com.sg/index.php?option