International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 2, Issue. 5, Sep.-Oct. 2012 pp-3943-3946 ISSN: 2249-6645

Resource and Quality Aware Location Anonymization Mechanism For Wireless Sensor Networks

Ch. Swarna Latha[1], D.T.V. Dharmajee Rao[2]
(M.Tech, Department of CSE, Aditya Institute of Technology and Management, Andhra Pradesh, India)
(Professor& HOD, Department of CSE, Aditya Institute of Technology and Management, Andhra Pradesh, India)

ABSTRACT: *A wireless sensor network is a heterogeneous network consisting of a large number of tiny low-cost nodes and one or more base stations. These networks can use in various applications like military, health and commercial. However, the privacy preservation problem has drawn huge attention in the research community. This problem is exacerbated in the domain of WSNs due to the extreme resource limitation of sensor nodes. In this paper, we proposed a model for privacy preservation for mobile users by using anonymization and aggregate location monitoring in a wireless sensor network. Resource-aware and quality-aware anonymization algorithms are designed to preserve personal location and provide location monitoring services. Sensor nodes execute location anonymization algorithms to provide k-anonymous aggregate locations. To evaluate the performance of the proposed algorithm we simulate it in the NS2 simulator. Our experimental results show that proposed solution provides high quality location monitoring services for end users and guarantees the location privacy of the monitored persons.*

Keywords: *Aggregate location, Anonymization, Cloaked area, Sensor node, WSN, NS2.*

I. Introduction

A wireless sensor network (WSN) is a heterogeneous network consisting of a large number of tiny low-cost nodes (devices) and one or more base stations (sinks) [1]. Main purpose of the WSN is to monitor some physical phenomena (e.g., temperature, barometric pressure, light) inside an area of deployment. Nodes are equipped with radio transceiver, processing unit, battery and sensor(s). Nodes are constrained in processing power and energy, whereas the base stations are not severely energy resources. The base station act as gateways between the WSN and other networks such as Internet etc.. The WSN is used in various applications like military, health and commercial. WSNs are becoming one of the building blocks of pervasive computing. They provide simple and cheap mechanism for monitoring in the specified area. But WSN technology is an inappropriate use can significantly violate privacy of humans. WSNs are frequently deployed to collect sensitive information. WSN can be used to monitor the movements of traffic in a city. Such a network can be used to determine location of people or vehicles [2].

If this information is available on a wide basis it can easily lead to blackmailing or stalking. It can be also exploited by terrorists as a targeting tool to impact specific people or buildings. Another example of a WSN application, in which privacy is heavily exposed, is health monitoring. Here, the medical measurements should be available only to the attending physician [4,5]. Wrong usage of simple commercial WSNs can easily result into serious privacy violations as well. Suppose that the WSN monitors people movements at a supermarket to improve the placement of products within the shelves. If someone is able to find out detailed information related to a particular person, then a seemingly innocent application turns into a privacy violating tracking device. This example demonstrates that in most cases collected data they do not pose a privacy threat. The problem arises when the data can be linked to a specific person. This is why anonymity and proper identity management of the nodes, or their carriers, or the subjects that these nodes monitor, are needed. If an attacker is not able to link measured data with the measuring device or location then this data is of a little value for privacy attacks [6].

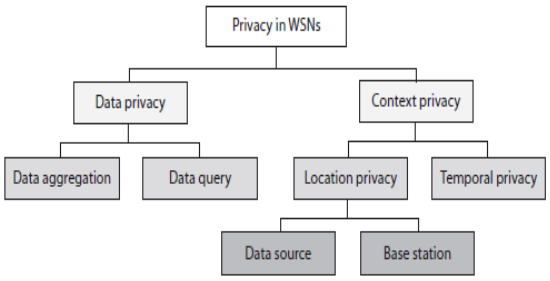

Fig 1: privacy preserving protections in WSNs

Privacy in the WSN is classified into Data-oriented and Context-oriented [3]. Data-oriented protections are then categorized into data aggregation and data query techniques. Context-oriented privacy protections can be split into location privacy and temporal privacy techniques, the location privacy is split into data source and base station techniques which is described in figure 1.

In this paper, we propose a privacy preservation of such mobile users with the help of anonymization and by reporting aggregate location. An anonymization means a person is indistinguishable amongst k persons in a network. The most effective way to compromise location privacy used by adversary is packet-tracing. In such an attack, an adversary can locate the immediate nodes by eavesdropping the transmitted packet, and further reduce the flow direction of packets. Even worse, the attacker can trace hop-by-hop towards the sink or source nodes. To defend against packet-tracing attack, many approaches are proposed. One of the approaches is providing aggregate location of a user. Along with privacy preservation of mobile users we are monitoring location of any mobile user through our system. Location monitoring is defined as monitoring every action, movement of any mobile user without disturbing its privacy.

The rest of the paper is organized as section 2: discuss about the related work, section 3: presents the Proposed Model, section 4: discuss about Proposed

Solution, section 5: discuss about Experimental setup, section 6: concludes the paper.

II. Related Work

Chaum [11] has started developing solutions for anonymous communications to provide privacy in WSNs. It is used to provide users with an anonymous e-mail system based on a special type of device called the mix. The main functionality of a mix is to receive a cryptographically encrypted message and transform it into a new message indistinguishable from the originally input one. In order to send a message, the source creates several layers of encryption over the message using the public keys of the different mixes that the message will traverse. Onion routing [9] and Tor [7] provide application independent anonymous connections in near real time by creating connections through a set of machines called the onion routers. Whenever an application establishes a connection, it first connects to an onion proxy, which is the entrance point to the anonymous network. The onion proxy is in charge of determining a series of onion routers that will define the bidirectional path that the packets of that specific connection will traverse. The path is constructed by using the cryptographic material of each of the onion routers, which is included in a data structure called the onion. Once the path has been established, the application data is sent through the onion network by adding a layer of encryption for each of the hops in the anonymous path. Each of the onion routers peels of its corresponding layer, changing the appearance of the data, and forwards it to the next onion router. The main drawback of this technique is based on a network core which the users must fully trust. Later Crowds [10] and Hordes [8] were proposed decentralized approaches. Both approaches are based on the idea of making individuals disappear into a group of peers. Upon receiving a message from a peer, the recipient will randomly choose whether to forward it to another peer or to finally submit it to the real destination. Each member of the path must remember its predecessor and successor so that subsequent messages coming from the same source follow the same path through the anonymous network. Note that any member of the path has only a local view of the route that a message traverses so that no peer can determine who the actual origin of a message is. Furthermore, since all communications are re-encrypted at every hop, a local eavesdropper cannot easily determine the destination of a message unless the originator decides to send the message directly to the destination. The main difference between Crowds and Hordes is in the way responses are sent back to the origin. In Hordes it is done by multicasting messages, which provides a better performance.

III. Proposed Model

The proposed Architecture consists of user, server and trusted zone and Sensor node, mobile users in a trusted zone. Anonymity level is set by administrator of a system to provide security for mobile users in a trusted zone. The mobility objects are shown in figure 2 by green color. If a user asks query regarding any user in a zone to a server then server passes this query to a sensor nodes present in trusted zone. Then sensor node from one area will exchange message with the other and report an aggregate location to the server and then server will send the answer to the user.

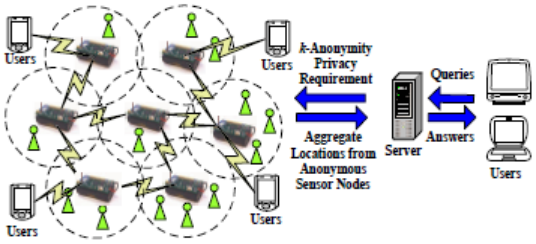

Fig 2: Proposed Architecture

IV. Proposed Solution

In our proposed solution we propose two algorithms

4.1 Resource aware algorithm

The main idea of the Resource aware algorithm is to find adequate number of persons in that network and accordingly finding a cloaked area as MBR (minimum bounded area).

Broadcast step

In this step, every sensor node in a network broadcasts a message which contains id, area and number of nodes to its nearest neighbor. In this way every sensor node forms its own table and also checks for adequate number of objects in its sensing area and accordingly it sends notification message to the nearer sensor nodes and follows the next step.

Cloaked area step

The basic idea of this step is that each sensor node blurs its sensing area into a cloaked area that includes at least k objects, in order to satisfy the k-anonymity privacy requirement. To minimize computational cost, it uses a greedy approach to find a cloaked area based on the information stored in table. Each sensor node initializes a set S and then determines a score for each peer in its table. The score is defined as a ratio of the object count of the peer to the distance between the peer and node. The score is calculated to select a set of peers from table 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 table to S until S contains at least k objects. Finally, node determines the cloaked area that is a minimum bounding rectangle that covers the sensing area of the sensor nodes in S, and the total number of objects in S.

Validation step:

Validation step is used to avoid reporting aggregate locations with a containment relationship to the server. We do not allow the sensor nodes to report their aggregate locations with the containment relationship to the server, because combining these aggregate locations may pose privacy leakage.

4.2 Quality aware algorithm

The quality-aware algorithm starts from a cloaked area A, which is computed by resource aware algorithm. Then A will be iteratively updated 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.

Search space step

Sensor network has a large number of sensor nodes hence it is very costly for a sensor node to gather the information of all the sensor nodes to compute its minimal cloaked area. To reduce the cost, node determines a search space based on the input cloaked area computed by the resource-aware algorithm.

The Minimal Cloaked Area step

This step takes a set of peers residing in the search space, S, as an input and computes the minimal cloaked area for the sensor node m. The basic idea of the first optimization technique is that we do not need to examine all the combinations of the peers in S, instead we only need to consider the combinations of at most four peers. Because at most two sensor nodes defines width of MBR and at most two sensor nodes defines height of MBR. It reduces cost by reducing the number of MBR computations among the peers in S. The second optimization technique has two properties, lattice structure and monotonicity property. In a lattice structure, a data set that contains n items can generate 2^{n-1} item sets excluding a null set. We generate the lattice structure from the lowest level based on a simple generation rule. The monotonicity property of a function f indicates that if X is a subset of Y, then f(X) must not exceed f(Y).

For our problem, the MBR of a set of sensor nodes S has the monotonicity property, because adding sensor nodes to S must not decrease the area of the MBR of S or the number of objects within the MBR of S.

The validation step

This step is to avoid reporting aggregate locations with a containment relationship to the server. We do not allow the sensor nodes to report their aggregate locations with the containment relationship to the server, because combining these aggregate locations may pose privacy leakage.

V. Experimental Setup

We have implemented our proposed algorithm in NS2, which has been highly validated by the networking research community. The simulation parameters where listed in table 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 $N^{\wedge}$ in a sensor node's sensing area and the actual one N.

Table 1: NS2 parameters

Parameters	Value
MAC Layer	IEEE 802.11
Number of nodes	20
Data rate	11Mbps
Packet Size	512 B
Simulation Duration	200 sec
Traffic Flow	TCP

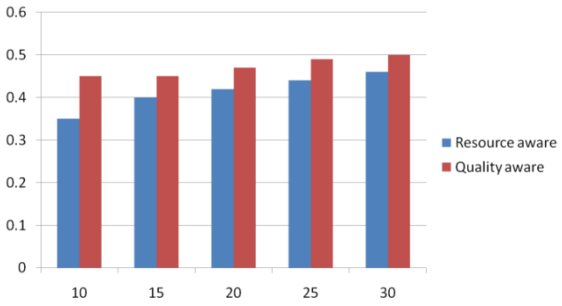

Fig 3: Attack model error vs anonymity levels

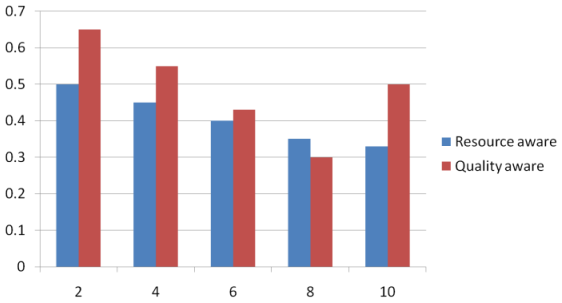

Fig 4: Attack model error vs number of objects in (thousands)

Figure 3 depicts that the stricter the anonymity level, the larger the attacker model error will be encountered by an adversary. When the anonymity level gets stricter, our algorithms generate larger cloaked areas, which reduce the accuracy of the aggregate locations reported to the server. Figure 4 shows that the attacker model error reduces, as the number of objects gets larger. This is because when there are more objects, our algorithms generate smaller cloaked areas, which increase the accuracy of the aggregate locations reported to the server. It is difficult to set a hard quantitative threshold for the attacker model error.

VI. Conclusion

A wireless sensor network is a heterogeneous network consisting of a large number of tiny low-cost nodes and one or more base stations. The privacy preservation problem has drawn huge attention in the research community. This problem is exacerbated in the domain of WSNs due to the extreme resource limitation of sensor nodes. To overcome privacy problem in WSN, we proposed a model for privacy preservation for mobile users by using anonymization and aggregate location monitoring in a wireless sensor network. Resource-aware and quality-aware anonymization algorithms are designed to preserve personal location and provide location monitoring services. Sensor nodes execute location anonymization algorithms to provide k-anonymous aggregate locations. To evaluate the performance of the proposed algorithm we simulate it in the NS2 simulator. Our experimental results show that proposed solution provides high quality location monitoring services for end users and guarantees the location privacy of the monitored persons.

References

[1] D. Culler and M. S. Deborah Estrin, .Overview of sensor networks, IEEE Computer, 2004.

[2] M. Gruteser, G. Schelle, A. Jain, R. Han, and Grunwald , Privacy-aware location sensor networks, 2003.

[3] W. He, X.Liu, H. Nguyen, K. Nahrstedt and Abdelzaher, PDA: Privacy-preserving data aggregation in wireless sensor networks, IEEE, 2007.

[4] C.-Y. Chow, M. F. Mokbel, and X. Liu, .A peer-to-peer spatial cloaking algorithm for anonymous location-based services,. In Proc. of ACM GIS, 2006.

[5] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias "Preventing location-based identity inference in anonymous spatial queries" IEEE,2007.

[6] B.Son, S. Shin, J.Kim and Y.Her "Implementation of the Real-Time People Counting System using Wireless Sensor Networks," IJMUE, 2007.

[7] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In SSYM'04: Proceedings of the 13th conference on USENIX Security Symposium, pages 21{21, Berkeley, CA, USA, 2004.

[8] B. N. Levine and C. Shields. Hordes: "A Multicast Based Protocol for Anonymity". IEEE International Conference, 2002.

[9] M. Reed, P. Syverson, and D. Goldschlag. Anonymous Connections and Onion Routing. Selected Areas in Communications, IEEE Journal on, May 1998.

[10] M. Reiter and A. Rubin.Crowds: Anonymity for Web Transactions. ACM transactions on information and system security, 1998.

[11] Y. Ouyang, Z. Le, Y. Xu, N. Triandopoulos, S. Zhang, J. Ford, and F. Makedon. "Providing Anonymity in Wireless Sensor Networks", IEEE International Conference July 2007.