ISSN:2249-5789
Irrinki Mohana Krishna et al , International Journal of Computer Science & Communication Networks,Vol 2(5), 623-627

QOS Aware Location Anonymization Mechanism for Wireless Sensor Networks

Irrinki Mohana Krishna[1], *Kothapalli Ramesh*[2]

*(M.Tech, Department of CSE, Kakinada Institute of Engineering & Technology, Andhra Pradesh, India)

*(Assistant professor, Department of CSE, Kakinada Institute of Engineering & Technology, Andhra Pradesh, India)

Abstract

To provide privacy in the location monitoring system in wireless sensor networks, in this paper we propose a frame work based on the location anonymization algorithms such as Resource and Location aware algorithms to provide efficient location monitoring system users. These algorithms are based on the K-anonymity privacy concept. The goal of resource aware algorithm is to minimize communication cost, and quality-aware algorithm increases the efficiency of the aggregate locations by decreasing the size of monitoring area. A spatial histogram method is used to measure the distribution of the monitored persons based on aggregate location information and the estimated distribution is used to provide location monitoring services through answering range queries. 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: Anonymization, Cloaked area, Sensor node, WSN, NS2.

1. Introduction

Now a days the world is expected to be offering numerous opportunities both to industry and end users. In this situation, man is completely depend upon the technology to perform his works, everyday objects will be fitted with computational and sensing capabilities. To achieve the circumstances we need to face many challenges. Among them we deem critical the ability to integrate different supporting technologies in such a way that they can provide an adequate level of security to the services being offered and to the data traversing the network. Well-known security and privacy problems already exist in current networks, hence, the creation of a trustworthy and resilient network as a conglomerate of networks and services might be unlikely if both security and privacy are not taken into consideration in advance [2].

Wireless Sensor Networks are ad hoc networks consist of tiny sensor nodes which are able to monitor the changes occur in its range [1]. These nodes can communicate with each other in a hop-by-hop fashion and sink collects and analyses the received data. Sensor nodes are extremely constrained in terms of processing, storing and communicating capabilities and battery supply. Resource limitation makes sensor nodes extremely vulnerable to different types of threats and attacks [12]. Privacy preserving techniques are classified into data-oriented and context-oriented. Data-oriented protections are then categorized into privacy protections during data aggregation and private data query techniques. Context-oriented privacy protections can be split into location privacy preserving techniques, that cover data source location protections and sink location protections, and temporal privacy preserving techniques [4,5,6].

Data privacy protections target privacy of data collected by a network and queries posted to a network. There are two types of adversaries threatening the data privacy external adversary and internal adversary. The external adversary only eavesdrops communication in a network. This kind of adversary can be easily defeated by encryption techniques such as SPINS or pDCS. On the other hand, the internal adversary controls one or more nodes and usually has an access to encryption keys of these nodes. In such a case, the easiest way to protect privacy of data sent from nodes to the base station is to use end-to-end encryption based on keys shared between the sending node and the base station. However, such encryption makes data aggregation

within the network impossible. Therefore, one of the challenges is to provide secure and privacy preserving data aggregation in the presence of an internal adversary.

Even though data privacy might be sufficiently protected, a sensor network may still leak valuable context-oriented information. Typical context-oriented information is information on source location, sink location and timing of events. This kind of information can be usually obtained by an external adversary using traffic analysis techniques.

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.

2. 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.

3. Proposed Model

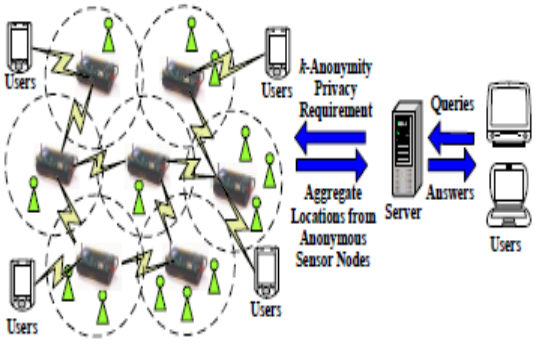

Fig 1: Proposed Architecture

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.

4. 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 2n-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.

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.

5. 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^ 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	100
Data rate	10Mbps
Packet Size	1024 B
Simulation Duration	300 sec
Traffic Flow	CBR

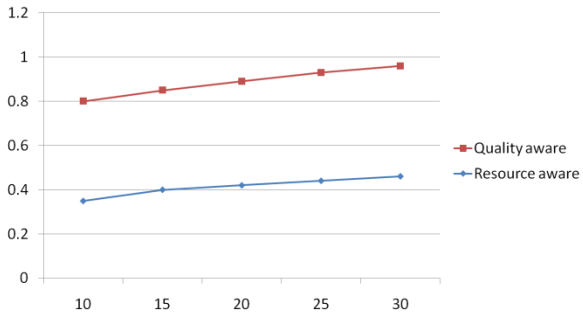

Fig 2: Attack model error vs anonymity levels

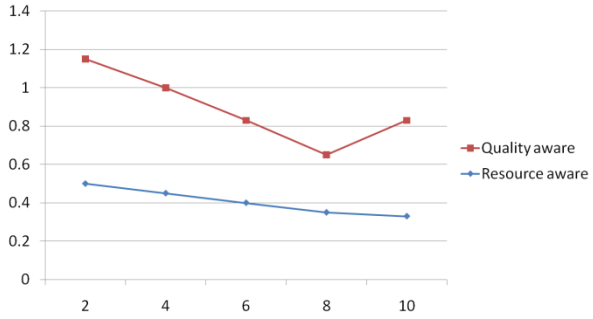

Fig 3: Attack model error vs number of objects in (thousands)

Figure 2 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 3 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.

6. Conclusion

To provide privacy in the location monitoring system in wireless sensor networks, in this paper we propose a frame work based on the location anonymization algorithms such as Resource and Location aware algorithms to provide efficient location monitoring system users. These algorithms are based on the K-anonymity privacy concept. The goal of resource aware algorithm is to minimize communication cost, and quality-aware algorithm increases the efficiency of the aggregate locations by decreasing the size of monitoring area. A spatial histogram method is used to measure the distribution of the monitored persons based on aggregate location information and the estimated distribution is used to provide location monitoring services through answering range queries. 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.
[12] J. Walters, Z. Liang, W. Shi, and V. Chaudhary. Security in Distributed, Grid, Mobile, and Pervasive Computing, chapter Wireless Sensor Network Security: A Survey, pages 367{411. Auerbach Publications, 2007.