Privacy Preservation Simulation and 3D Space Location Monitoring System Objects for Wireless Sensor Networks

Dr. Sudhir Dawra¹ & Rohit Kumar²
¹Professor, Ideal Institute of Technology, Ghaziabad
²Research Scholar, Sunrise University, Alwar.

Abstract: Monitoring private locations with a potentially insecure server poses security threats to the monitored individuals. To this end, we propose a privacy-preserving location monitoring system for wireless sensor networks in 3D Space. In our system, we are using two in-network location anonymization algorithms, namely, resource and quality-aware algorithms, which aim to enable the system to provide high-quality and secure location monitoring services for users, while preserving privacy. Algorithms rely on the well-established k-anonymity privacy concept, that is, a person is indistinguishable among k persons, to enable trusted sensor nodes to provide the aggregate location information of monitored persons for our system. 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. We will evaluate our system through simulated experiments.

Index Terms—Location privacy, wireless sensor networks, location monitoring system, aggregate query processing.

1. Introduction

The advance in wireless sensor technologies has resulted in many new applications for military and/or civilian purposes. Many cases of these applications rely on the information of personal locations, for example, surveillance and location systems. These location-dependent systems are realized by using either identity sensors or counting sensors. For identity sensors, for example, Bat [1] and Cricket [2], each individual has to carry a signal sender/receiver unit with a globally unique identifier. With identity sensors, the system can pinpoint the exact location of each monitored person. On the other hand, counting sensors, for example, photoelectric sensors [3], [4], and thermal sensors [5], are deployed 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 [2], [6], [7], [8]. 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 [8], [9], has been suggested as an effective approach to preserve location privacy [6], [8], [9]. Although the counting sensors by nature provide aggregate location information, they would also pose privacy breaches.

Fig. 1 gives an example of a privacy breach in a location monitoring system with counting sensors. There are 11 counting sensor nodes installed in nine rooms R1 to R9, and two hallways C1 and C2 (Fig. 1a). The nonzero number of persons detected by each sensor node is depicted as a number in parentheses. Figs. 1b and 1c give the numbers reported by the same set of sensor nodes at two consecutive time instances, respectively. If R3 is Alice’s office room, an adversary knows that Alice left R3 at time tiþ1 and went to C2 by knowing the number of persons detected by the sensor nodes in R3 and C2. Likewise, the adversary can infer that Alice left C2 at time tiþ2 and went to R7. Such knowledge leakage may lead to several privacy threats. For example, knowing that a person has visited certain clinical rooms may lead to knowing her health records. Also, knowing that a person has visited a certain bar or restaurant in a mall building may reveal confidential personal information.

This paper proposes a privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services[9]. Our system relies on the well-established k-anonymity privacy concept, which requires each person is indistinguishable among k persons. In our system, 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.
It is important to note that the value of k achieves a
trade-off between the strictness of privacy protection
and the quality of monitoring services. A smaller k
indicates less privacy protection, because a smaller
cloaked area will be reported from the sensor node;
hence better monitoring services. However, a larger
k results in a larger cloaked area, which will reduce
the quality of monitoring services, but it provides
better privacy protection. Our system can avoid the
privacy leakage in the example given in Fig. 1 by
providing low-quality location monitoring services
for small areas that the adversary could use to track
users, while providing high-quality services for
larger areas. The definition of a small area is relative
to the required anonymity level, because our system
provides better quality services for the same area if
we relax the required anonymity level. Thus, the
adversary cannot infer the number of persons
currently residing in a small area from our system
output with any fidelity; therefore, the adversary
cannot know that Alice is in room R3.

To preserve personal location privacy, we propose
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[10][11]. 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.
Although our system only knows the aggregate
location information about the monitored
persons, it can still provide monitoring services
through answering aggregate queries, for example, 
“What is the number of persons in a certain area?”
To support these monitoring services, we propose a
spatial histogram that analyzes the gathered
aggregate locations to estimate the distribution of the
monitored persons in the system. The estimated
distribution is used to answer aggregate queries.

We evaluate our system 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 percent) than the
resource-aware algorithm (the average accuracy is
about 75 percent). 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.

The rest of this paper is organized as follows: Our
system model is outlined in Section 2. Section 3
presents the resource and quality-aware location
anonymization algorithms. Section 4 describes the
aggregate query processing. Finally, Section 5
concludes the paper.

2. System Model

Figure 2, 3 describe the architecture design of
system, which consists 3 major entities one is System
server, server and sensor nodes.

C.Y. Chow etal defines the crisis addressed by
system, and then explains the detail of each
individual and the privacy model of the system.
Every sensor blurs its sensing area in this system,
to an area which is termed as cloaked area, in the
lying system at least k number of objects must be
presently residing. Every sensor node sends
information of aggregate location, which is known as
a cloaked area. The cloaked area consist the quantity
of persons or objects, this number is represented by
N and it is residing in sensing area of each sensor
node but only for the condition where \( N \geq K \).

Fig. 2 System Architecture: 1

The system architecture depicts the sensor node like S1, S2 to Sn and its sensing area like a1, a2 to an respectively. Along with a moving object O1, O2 to On. It requires a minimum anonymity level K. A aggregate location is found in set of area \( A_i=\) (Area i, Ni) where Area i represents a rectangular area and Ni represents number of objects present in that the sensing area of sensor such like \( Ni \geq K \). Ni = \( \bigcup \{j \mid O_j \; \subseteq S_i, \; 1 \leq j \leq n, \; \text{and} \; 1 \leq i \leq m, \; \text{and} \; 2 \} \). Spatial histogram is used to respond an aggregate query Q that asks regarding the number of objects in definite area Q. This area is based on the aggregate locations conceived from the sensor nodes.

The rival cannot identify the object’s accurate location because this system only tells about aggregate k-anonymous location information.

3. Proposed System

Our system proposed wireless sensor networks (WSN) by using a privacy-preservation location monitoring system to preserve the privacy of spatial monitored objects and to provide monitoring services. This system uses well established k-anonymity privacy concept. In this method, each sensor make a cloaked area by making blurs its sensing area, where at least k objects are living. Cumulative location information is reported by each sensor, which make a form of 3D cloaked sensing area, A, beside with the number of objects or persons, N, Situated in Area A. Here a middle tier entity called Containment-Resolver is proposed which accepts the information of aggregate location for monitored objects from the sensor nodes and after resolving containment, sends this resolved information to the server with no. of K-Failures. It is note worthy to take a note on the value of k accomplishes a difference between the firmness of privacy protection and the worth of monitoring services. If a smaller cloaked area reported by the sensors ,it represent a lesser value of k which indicate less privacy preservation as a minor cloaked area is reported by the sensors ,therefore it increase monitoring service to that area. In contrast a large value of k decrease the quality of monitored area service but improve the privacy of the objects or persons and obviously privacy protection. By using this system we can avoid the privacy leakage by providing low quality monitoring services for small areas whereas for large areas we will provide a good quality monitoring service so that the rival cannot abuse or track the user. This proposed system also considers the Z co-ordinate for cloaking the area in spatial systems (e.g. Multi-floor Buildings) to preserve the privacy. This also results in high privacy as compare to the privacy provided by the systems that uses the cloaking area shown by only X and Y coordinates (i.e. cloak the area of the same floor only) to preserve the privacy.

4. Key Features of Proposed Work

The Cost of communication for 3D resource aware location algorithm is low as compared to the other algorithm like 3D quality aware algorithm by considering the number of bytes and data by the sensor node for par phase of reporting. The quality of aggregate location information can be measured by the size of Cloaked Area accounted with the help of the sensors. As lesser cloaked area it improved accuracy of the aggregate location. The 3D quality-aware algorithm assures less cloaked area size compared to the 3D resource-aware algorithm. Containment resolution by Max-Object count algorithm reports less K-Failures as compared to containment resolution by Average-Object count algorithm.

The proposed 3D privacy-preserving location monitoring system for WSN can use the Z-coordinate also to show the cloaking area instead of using only X and Y coordinates. This means the system can cloak the area of different floors and can be used to protect the privacy of monitored objects in multi-floor buildings. Z -Coordinate is not considered in current experiment. Considers the Z-Coordinate this means we can use the system for Multi floor buildings.
Show the system in 3D. A middle-tier entity called Containment-Resolver is proposed to resolve the containment. 3D histogram will be used to show the distribution of objects for answering the user queries i.e. to provide the monitoring services.

**Features of the proposed system**
- Preserves privacy of moving objects
- Provides monitoring services
- Can vary no. of objects in system an cloak the area of different floors (Z-coordinate is used)

**Scope**
Evaluate the performance of location anonymization algorithms, namely 3D Resource-Aware algorithm and 3D Quality-Aware algorithm in spatial systems (specifically multi-floor buildings) in very dense environment, sparse environment and in general environment. Also evaluate the performance of Containment Resolution by Max-Object Count algorithm and Containment Resolution by Average-Object Count algorithm in all above three environments.

**Goals and Objectives**
- Understand the limitations of 2D privacy-preserving location monitoring system for WSN (Wireless Sensor Network).
- Understand the limitations of 3D privacy-preserving based on location monitoring for WSN (wireless sensor networks) used in multi-floor buildings.

**Primary Objectives**
- To evaluate the performance of 3D Resource-Aware algorithm in spatial systems (specifically multi-floor buildings) in very dense environment, sparse environment and in general environment.
- To evaluate the performance of 3D Quality-Aware algorithm in spatial systems (specifically multi-floor buildings) in very dense environment, sparse environment and in general environment.
- To evaluate the performance of Containment Resolution by Max-Object Count Algorithm in very dense environment, sparse environment and in general environment.
- To evaluate the performance of Containment Resolution by Average-Object Count Algorithm in very dense environment, sparse environment and in general environment.

**Secondary Objectives**
- Compare the performance of 3D Resource-Aware algorithm and 3D Quality-Aware algorithm in various environments.
- Compare the performance of Containment Resolution by Max-Object Count Algorithm and Containment Resolution by Average-Object Count Algorithm in various environments.

**Constraints**
- Area is fixed - System can be used only for buildings having rooms of similar size.
- No. of Sensor nodes and their positions are fixed
- Upper and lower limits to the no. of objects.

**Fig. 4 Simulation Modeling for 3D Privacy Preservation**

**Conclusion**
A 3D privacy preserving location monitoring system for wireless sensor networks is used to preserve the privacy of monitored objects in 3D space (e.g. multi-floor multi-section building) and to provide the monitoring services to the system users. The 3D resource-aware algorithm minimizes communication and computational cost, while the 3D quality-aware algorithm is used to maximize the accuracy of the aggregate locations by minimizing their monitored areas. 3D quality-aware algorithm requires very high MBR computations so its not efficient for WSNs established in 3D space. Since we are considering the X,Y and Z co-ordinate also to show the area which is being cloaked, we can use the system to preserve the privacy of monitoring objects in 3D space which is the new initiative in this area.

**Acknowledgment**
Authors like to thank Dr. V.K. Agarwal, Chancellor Sunrise University and Dr. Anup Pradhan, Director Research for providing research facilities in Sunrise University Campus.

**References**


