A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks

ANISETTI VANITHA NAGA JYOTHI

Dept of CS, SVKP & Dr K S Raju Arts & Science College, Penugonda, A.P, India,

K. LAKSHMANA REDDY

Associate Professor, Dept of CS, SVKP & Dr K S Raju Arts & Science College, Penugonda, A.P, India.

Abstract

Monitoring personal locations with a potentially untrusted server poses privacy threats to the monitored individuals. To this end, we propose a privacy-preserving location monitoring system for wireless sensor networks. In our system, we design two in-network location anonymization algorithms, namely, resource and quality-aware algorithms that aim to enable the system to provide high-quality location monitoring services for system users, while preserving personal location privacy. Both 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. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations by minimizing their monitored areas. To utilize the aggregate location information to provide location monitoring services, we use a spatial histogram approach that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then, the estimated distribution is used to provide location monitoring services through answering range queries. We evaluate our system through simulated experiments. The results show that our system provides high-quality location monitoring services for system users and guarantees the location privacy of the monitored persons.

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 and Cricket, each individual has to carry signal sender/receiver unit photoelectric sensors, and thermal sensors, are deployed to report the number of persons located in there with a globally unique identified. With identity sensors the system can pinpoint the exact location of each monitored person. On the other hand counting sensors, for example 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 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.

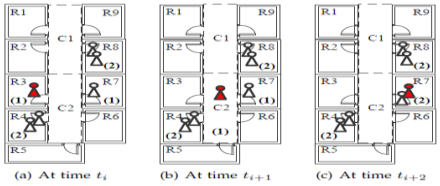

Fig. 1: A location monitoring system using counting sensors.

Fig 1.1 A location monitoring System Using Counting Sensors

Figure 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 the nonzero number of persons detected by each sensor node is depicted as a number in parentheses.

Figures 1b and 1c give the numbers reported by the same set of sensor nodes at two consecutive time instances ti+1 and ti+2, respectively. If R3 is Alice's office room, an adversary knows that Alice is in room R3 at time ti. Then the adversary knows that Alice left R3 at time ti+1 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 ti+2 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 the health records. Also, knowing that a person has visited a certain bar or restaurant in a mall building may reveal confidential personal information.

1.2 Purpose:

This proposes a privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services. 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, 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.

1.3 Scope:

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. 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

1.4 Motivation:

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 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

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

1.5 Overview:

We propose a privacy-preserving location monitoring system for wireless sensor networks. We design 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.

2. LITERATURE SURVEY

Straightforward approaches for preserving users' location privacy include enforcing privacy policies to restrict the use of collected location information and anonym zing the stored data before any disclosure. However, these approaches fail to prevent internal data thefts or inadvertent disclosure.

2.1 Location Anonymization:

In this techniques have been widely used to anonymization personal location information before any server gathers the location information, in order to preserve personal location privacy in location-based services. These techniques are based on one of the three concepts.

- **False locations** Instead of reporting the monitored object's exact location, the object reports in different locations, where only one of them is the object's actual location while the rest are false locations.
- **Spatial cloaking** the spatial cloaking technique blurs a user's location into a cloaked spatial area that satisfies the users specified privacy requirements.
- **Space transformation**. This technique transforms the location information of queries and data into another space, where the spatial relationship among the query and data are encoded. Among these three privacy concepts, only the spatial cloaking technique can be applied to our problem.

Disadvantage:

- The false location techniques cannot provide high quality monitoring services due to a large amount of false location information
- The space transformation techniques cannot provide privacy-preserving monitoring services as it reveals the monitored object's exact location information to the query issuer
- The spatial cloaking techniques can provide aggregate location information to the server and balance a trade-off between privacy protection and the quality of services by tuning the specified privacy requirements.

2.2 A Peer to peer Spatial Cloaking:

A peer-to-peer (P2P) spatial cloaking algorithm in which mobile and stationary users can entertain location-based services without revealing their exact location information. The main idea is that before requesting any location-based service, the mobile user will form a group from her peers via single-hop communication and/or multi-hop routing. Then the spatial cloaked area is computed as the region that covers the entire group of peers.

Two modes of operations are supported within the proposed P2P spatial cloaking algorithm, namely, the on-demand mode and the proactive mode Experimental results show that the P2P spatial cloaking algorithm operated in the on-demand mode has lower communication cost and better quality of services than the proactive mode, but the on-demand incurs longer response time.

Disadvantage:

- It suffers from a longer response time than the algorithm operated in the proactive mode.
- It generally incurs higher communication overhead and gives lower quality of service than the on-demand mode

3. SYSTEM ANALYSIS

3.1 Existing system:

Straightforward approaches for preserving users' location privacy include enforcing privacy policies to restrict the use of collected location information anonym zing the stored data before any disclosure. However, these approaches fail to prevent internal data thefts or inadvertent disclosure. Recently, location anonymization techniques have been widely used to anonymization personal location information before any server gathers the location information, in order to preserve personal location privacy in location-based services. These techniques are based on one of the three concepts.

- False locations. Instead of reporting the monitored object's exact location, the object reports n different locations, where only one of them is the object's actual location while the rest are false locations.
- Spatial cloaking. The spatial cloaking technique blurs a user's location into a cloaked spatial area that satisfies the user's specified privacy requirements.
- Space transformation. This technique transforms the location information of queries and data into another space, where the spatial relationship among the query and data are encoded.

Among these three privacy concepts, only the spatial cloaking technique can be applied to our problem. The main reasons for this are that (a) the false location techniques cannot provide high quality monitoring services due to a large amount of false location information; (b) the space transformation techniques cannot provide privacy-preserving monitoring services as it reveals the monitored object's exact location information to the query issuer; and (c) the spatial cloaking techniques can provide aggregate location information to the server and balance a trade-off between privacy protection and the quality of services by tuning the specified privacy requirements, for example, k-anonymity and minimum area privacy requirements. Thus we adopt the spatial cloaking technique to preserve the monitored object's location privacy in our location monitoring system.

3.2 Disadvantages:

- The false location techniques cannot provide high quality monitoring services due to a large amount of false location information;
- The space transformation techniques cannot provide privacy-preserving monitoring services as it reveals the monitored object's exact location information to the query issuer;
- The spatial cloaking techniques can provide aggregate location information to the server and balance a trade-off between privacy protection and the quality of services by tuning the specified privacy requirements

3.3 Proposed System:

We design 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, we propose 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. We evaluate our system through simulated experiments. The results show that our system provides high quality location monitoring services (the accuracy of the resource-aware algorithm is about 75% and the accuracy of the quality aware algorithm is about 90%), while preserving the monitored object's location privacy.

3.4 Advantages:

- To provide location monitoring services based on the aggregate location information.
- 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.

4. OUTPUT SCREEN SHOTS

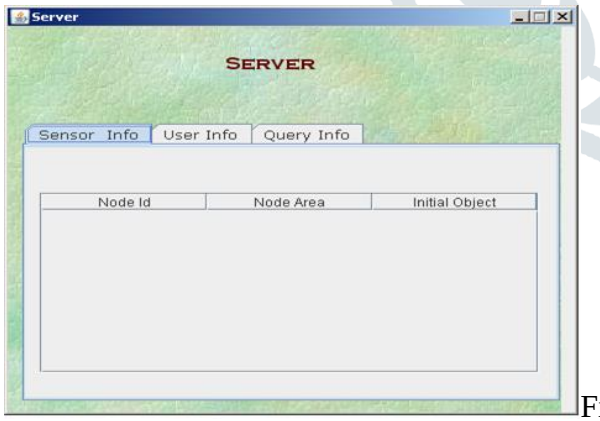

Fig 4.1: First run the sensor

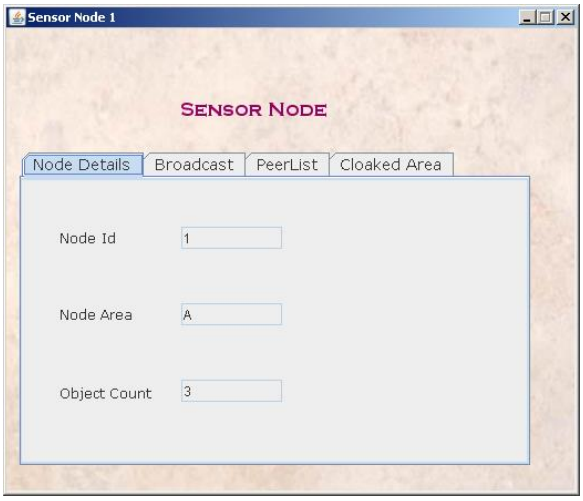

Fig 4.2: Run Sensor

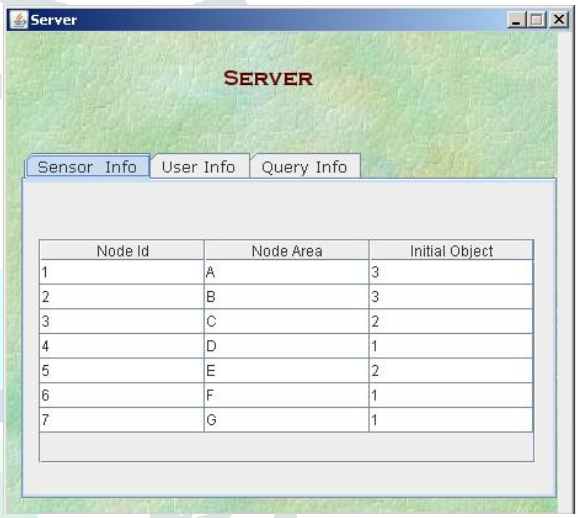

Fig 4.3: server window

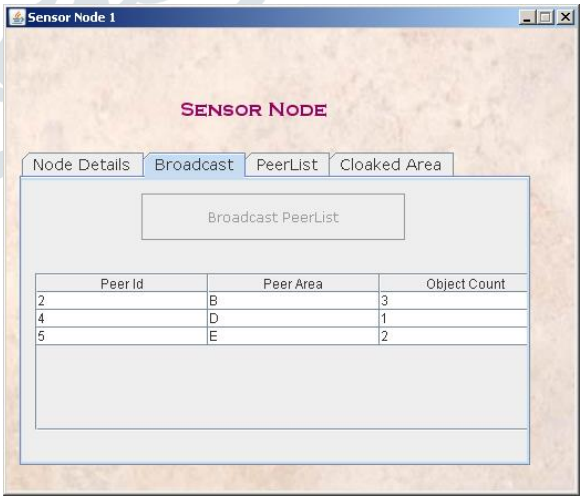

Fig 4.4 Broadcast of Sensor Node1

5. CONCLUSION

We propose a privacy-preserving location monitoring system for wireless sensor networks. We design 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, we propose 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. We evaluate our system through simulated experiments. The results show that our system provides high quality location monitoring services (the accuracy of the resource-aware algorithm is about 75% and the accuracy of the quality aware algorithm is about 90%), while preserving the monitored object's location privacy.

6. REFERENCES

[1] A. Harter, A. Hopper, P. Staggers, A. Ward, and P. Webster, .The anatomy of a context-aware application,. in Proc. of Modicum, 1999.

[2] N. B. Priyanta A.Chakraborty, and H.Balakrishnan, .The cricket location-support system,. in Proc. of Mobi Com, 2000.

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

[4] Onesystems Technologies, .Counting people in buildings. http://www.onesystemstech.com.sg/index.php?option=com content&task=view%&id=10..

[5] Traf-Sys Inc., .People counting systems. http://www.trafsys. com/products/people-counters/thermal-sensor.aspx..

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

[7] G. Kaupins and R. Minch, .Legal and ethical implications of employee location monitoring,. in Proc. of HICSS, 2005.

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

[9] .Title 47 United States Code Section 222 (h) (2),http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname= browse usc&do%cid=Cite:+47USC222..

About Authors:

ANISETTI VANITHA NAGA JYOTHI is currently pursuing CS SVKP & Dr K S Raju Arts & Science College, Penugonda, West Godavari A.P. His research interests include Data Mining, Artificial Intelligence.

K.Lakshmana Reddy is working as an Associate Professor in the Department of Computer Science in SVKP & Dr K S Raju Arts &Science College, Penugonda, A.P. He received MCA from Andhra University, 'C' level from DOEACC, New Delhi and M.Tech from Acharya Nagarjuna University, A.P. He attended and presented papers in conferences and seminars. He has done online certifications in several courses from NPTEL. His areas of interests includes Computer Networks, Network Security and Cryptography, Formal Languages and Automata Theory and Object Oriented programming languages.