International Journal of Advanced Computer and Mathematical Sciences
ISSN 2230-9624. Vol 3, Issue 3, 2012, pp 343-347
http://bipublication.com

# EXPLORING SECURED LOCATION DATA FOR PRESERVING IN SCANNING SYSTEM

**Nikhil Kumar Sanghvi**

Guru Nanak Engineering College, Hyderabad, AP, INDIA

[Received-09/09/2012, Accepted-25/09/2012]

**ABSTRACT:**

Monitoring services are provided by building wireless sensor networks for a High Secured Location Scanning System. A potentially un-trusted server with monitoring personal locations poses privacy threats to the monitored individuals. In this paper, we discuss about a well established k-anonymity privacy concept which requires each person, is indistinguishable among k persons relies upon our system. In our system, at least k persons are residing in each sensor node which blurs its sensing area into a cloaked area. Aggregate location information is reported by each sensor node. However, two in-network aggregate location anonymization algorithms are proposed namely, resource and quality-aware algorithms. The sensor nodes to collaborate with each other to blur their sensing areas into cloaked areas are required by both algorithms, such that each cloaked area contains at least k persons including a k-anonymous cloaked area. The main aim of resource-aware algorithm is to minimize computational cost and communication. The aim of Quality-aware algorithm is to minimize the size of the cloaked areas. Simulated experiments are evaluated through our system and our system provides high quality location monitoring services and guarantees the location privacy of the monitored persons are shown in our results.

**Keywords:** Monitoring Services, Wireless Sensor Networks, k-anonymity, Sensor nodes.

## INTRODUCTION:

A wireless sensor network consists of spatially tribute autonomous sensors to monitor physical or environmental conditions. Wireless sensor networks provide a simple, economic approach for the deployment of distributed monitor and control services. A wireless sensor network is a collection of small randomly dispersed devices that provide three essential functions; the ability to monitor physical and environmental conditions, often in real time,

such as temperature, pressure, light and humidity; the ability to operate devices such as switches, motors or actuators that control those conditions; and the ability to provide efficient, reliable communications via a wireless network. The wireless sensor network is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one or sometimes several sensors. The implementation of this last capability is the most unique to wireless sensor networks. Since they are designed for low traffic monitor and control applications, it is not necessary for them to support the high data throughput requirements that data networks like Wi-Fi require.

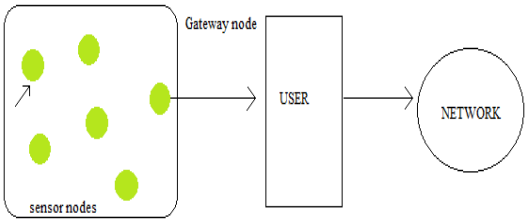


Fig 1. Wireless sensor networks.

The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. They are now used in many industrial and civilian application areas including industrial process monitoring and control machine health monitoring, healthcare applications and traffic control. With a globally unique identifier each individual has to carry a signal sender/receiver unit. Bat and Cricket are examples of identity sensors. The exact location of each monitored person with identity sensors is pinpointed by the system. On the other hand, to report the number of persons located in their sensing areas to a server is deployed by counting sensors, examples for counting sensors are thermal sensors and photoelectric sensors. With potentially un-trusted system poses privacy threats to the monitored individuals with monitoring personal locations, to infer personal sensitive information an adversary could abuse the location information gathered by the system. The concept of aggregate location information is used to tackle such a privacy breach, i.e. 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. A privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services are proposed in our paper. The well established

k-anonymity privacy concept, which requires each person, is indistinguishable among k persons relies upon our system. At least k persons are residing in each sensor node which blurs its sensing area into a cloaked area in our system. Fig2 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 M1 to M9, and two hallways A1 and A2. Each sensor node is depicted as a number in parentheses by the nonzero number of persons detected. Figures 2b and 2c give the numbers reported by the same set of sensor

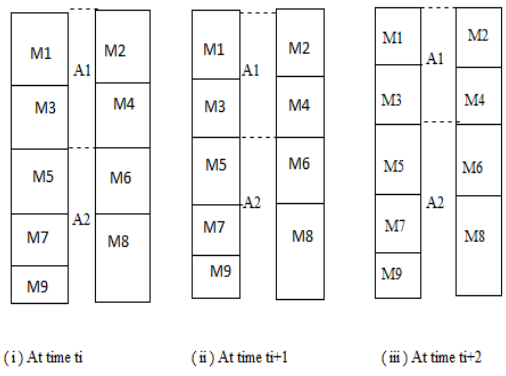


Fig 2. Location monitoring system

nodes at two consecutive time instances ti+1 and ti+2, respectively. If M3 is Anne's office room, an adversary knows that Anne is in room M3 at time ti. Then the adversary knows that Anne left M3 at time ti+1 and went to A2 by knowing the number of persons detected by the sensor nodes in M3 and A2. Likewise, the adversary can infer that Anne left A2 at time ti+2 and went to M7. 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. The Form of a cloaked area, C, along with the number of persons, P, located in C, where $P \geq k$, to the server. It is important to note that the quality of monitoring services and the strictness of privacy protection a trade-off and achieves the value of k. Because of a smaller cloaked area will be reported from the sensor node, a smaller k indicates less privacy protection and hence better monitoring services.

The main aim of resource-aware algorithm is to minimize computational cost and communication. While the main aim of quality-aware algorithm is 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. With the number of monitored persons in the area as an aggregate location

to the server the sensor node reports its cloaked area for both algorithms. It can still provide monitoring services through answering aggregate queries even though our system only knows the aggregate location information about the monitored persons. The quality-aware algorithm provides more accurate monitoring services than the resource-aware algorithm and the communication and computational cost of the resource-aware algorithm is lower than the quality-aware algorithm. The quality-aware algorithm is favorable for the system and the resource-aware algorithm is suitable for the system, since the sensor nodes have scare communication and computational resources and accuracy is the most important factor in monitoring services.

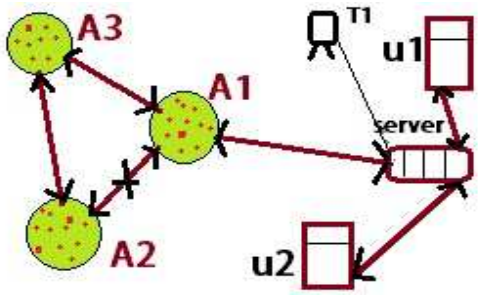


Fig 2. System architecture

Here A1,A2, A3 are Areas

u1,u2 are Users, T1- Tower

**SYSTEM MODEL**

The architecture of our system consists of three major entities they are sensor nodes, server and system users.

**Sensor nodes:** The number of objects in its sensing area, blurring its sensing area into a cloaked area C is determined by each sensor node which is responsible for it, and which includes at least k objects, and reporting C with the number of objects located in C as aggregate location information to the server. We do not have any assumption about the network topology, as our system requires a communication path from each sensor node to the server through a distributed tree. Each sensor node is aware of its location and sensing area.

**System users:** The server uses the spatial histogram to answer their queries. The server or the sensor nodes can issue range queries to our system through users and authenticated administrators.

**CONCLUSION:**

In this paper, we propose a High Secured Location Scanning system for wireless sensor networks. In this paper, we have discussed about a well established k-anonymity privacy concept which requires each person, is indistinguishable among k persons relies upon our system. However, two in-network aggregate location anonymization algorithms are proposed namely, resource and quality-aware algorithms. The sensor nodes to collaborate with each other to blur their sensing areas

into cloaked areas are required by both algorithms, such that each cloaked area contains at least k persons including a k-anonymous cloaked area. Simulated experiments are evaluated through our system and our system provides high quality location monitoring services and guarantees the location privacy of the monitored persons are shown in our results.

## REFERENCES:

[1] R. Matischek: "Real-Time Communication MAC Protocols for Wireless Sensor Networks", 2012, ISBN 978-3-8300-6349-0.

[2] Chi-Yin Chow, Student Member, IEEE, Mohamed F. Mokbel, Member, IEEE, and Tian He, Member, IEEE" A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 1, Jan 2011

[3] Ortolani, S.; Conti, M.; Crispo, B.; Di Pietro, R. World of Wireless, Mobile and Multimedia Networks" Events privacy in WSNs: A new model and its application" Publication Year: 2011 ,

[4] F. Viani, P. Rocca, M. Benedetti, G. Oliveri, A. Massa , "Electromagnetic passive localization and tracking of moving targets in a WSN-infrastructured environment " in Inverse Problems, vol. 26, (2010), p. 1-15. - DOI: 10.1088/0266-5611/26/7/074003

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

[6] Dargie, W. and Poellabauer, C., "Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010 ISBN 978-0-470-99765-9, pp. 168–183, 191–192 .

[7] Muaz Niazi, Amir Hussain (2011). A Novel Agent-Based Simulation Framework for Sensing in Complex Adaptive Environments. IEEE Sensors Journal, Vol.11 No. 2, 404–412.

[8] TinyOS Programming, Philip Levis, Cambridge University Press, 2009.

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

[10] J. Kong and X. Hong, .ANODR: Anonymous on demand routing with untraceable routes for mobile adhoc networks,. in *Proc. Of MobiHoc*, 2003.

[11] H. Kido, Y. Yanagisawa, and T. Satoh, .An anonymous communication technique using dummies for location-based services,. In *Proc. of ICPS*, 2005.

[12] 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.

[13] S. Guo, T. He, M. F. Mokbel, J. A. Stankovic, and T. F. Abdelzaher, .On accurate and efficient statistical counting in sensor-based surveillance systems,. in *Proc. of MASS*, 2008.

[14] K. Bohrer, S. Levy, X. Liu, and E. Schonberg, Individualized privacy policy based access control,.In *Proc. of ICEC*, 2003.

[15] E. Snekkenes, .Concepts for personal location privacy policies,. in *Proc. of ACM EC*, 2001.