Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Network Location and Data Anonymization Technique for Data Privacy in WSN

**P. Jaya Prakash**
*Assoc. Test Architect*
*India*

**B. Sunil Kumar***
*CSE Dept, JNIT,JNTUH*
*India*

**D. Kiran Kumar**
*CSE Dept, VBIT,JNTUH*
*India*

**T.P. SaraChandirka**
*CSE, SV College,Tirupathi*
*India*

***Abstract*— Wireless sensor technologies are utilizing in various real time location identification systems. Recently they are adopted as location dependent subsystems for Government, Civilian and Military applications to monitor location information and node movements. Monitoring the personal locations through an un trusted server poses the privacy threat for the monitored individuals. Adversary may get the monitored information from un trusted server and misuse it to know the sensitive personal information. To avoid these problems in wireless sensor networks in this paper we introduced the Network Location and Data Anonymization technique with K- anonymity concept. This concept preserves the privacy of monitored person's sensitive information in wireless sensor networks. In order to minimize the computation and location monitoring cost we deployed spatial histogram approach to the network server nodes. Our experiments with this approach on hospital management system, given the scalable results towards the aim.***

***Keywords*— wireless sensor networks, K- anonymity , data privacy, wireless network sensors .***

## I. INTRODUCTION

Wireless sensor networks (WSN) emerged as a resilience technology, which offers low cost, high bandwidth, trustable network services. They consist of accurate wireless sensor nodes and scalable multi hop routing protocols with the dedicated server environment. Many of the applications like video surveillance, node trackers and military applications are using location dependent sensors [1,2]. These are either identity or counter sensors to identify the exact location of each monitored person and to return the count of person's monitored. These sensors are deployed at various locations to monitor the node movements and to send a comprehensive information to the dedicated server. Users of this server may query to get any monitoring node information with location and movements as shown in below fig.1.

Our location monitoring system contained identity servers gives the comprehensive location information and node personal information to server. Unfortunately, monitoring the personal information from un trusted server may allow the adversary to abuse the personal sensitive information[3].To overcome this problem, in this paper we introduced the Network Location and Data Anonymization technique with K- anonymity concept. This concept preserves the privacy of monitored person's sensitive information in wireless sensor networks. In this approach we are aggregating the location and data information as related group information instead of individual node information and increasing the security of personal information through authorized access. Our system relies on complete reliable K-anonymity privacy concept and every sensor node blurs its sensing area called clocked area. We are deploying spatial histogram[7] to obtain the count of nodes and their related groups information.

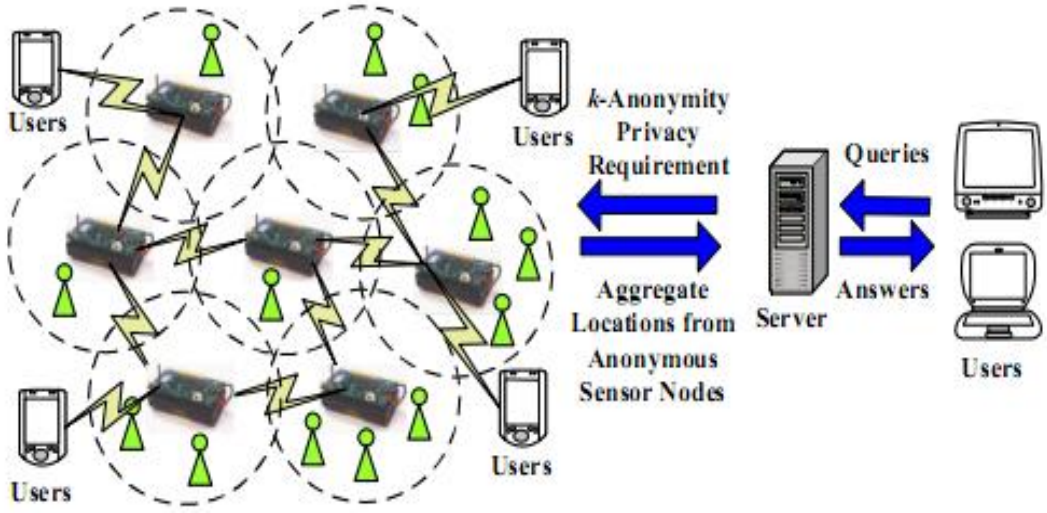


Fig.1. Distributed WSN Environment Model

 

## II. RELATED WORK

In order to count and track moving nodes, several systems [3],[5] are using image processing Technology by a digital camera . In order to process the image data, these Processing systems were based on movement analysis of moving nodes in deployed environment. Cathey and sierra developed an image processing system to find and monitor the moving people using a fixed video camera. The intention was only to identify the number of moving nodes by using the counting sensors [6].Their application not concerned on the goal of Location identification which is also required in information tracking. In their system, they captured the input form either recorded video or a stationary camera and the environment having trajectories which gives the spatiotemporal coordinates values of individual nodes as they move in the environment.

Byung and Syung in their research they extended the capabilities of this system, that does automatically counting the nodes and monitoring the environment by using laser-beam sensors. First, they implemented an automatic node counting system to count the number of Moving nodes in the selected environment using the laser-beam sensors. Later they extended this environment to monitor system based on a wsn in real experiments. This paper concerns on how protect the user sensitive information from an adversary attacks by using the K-anonymity algorithm to anonimyze all nodes information as group data and allows the data accessing through secure authentication.

## III. NETWORK LOCATION AND DATA ANONYMIZATION

Privacy for data concerns in location-dependent application is typically having a location broker, who exists in the middleware layer of that application. Due to the improvements in wireless sensor networking and location monitoring technologies location-dependent wireless network applications got inspired, but they also having some significant privacy risks due to lack of knowledge. Privacy can determined by privacy policies, that gives the information to the user about a service provider's data handling methodologies and helps as the basic for the application user's decision to free up the data. With the help of privacy policies, policy users may get interaction and partial protection from malicious service providers. This paper concerns privacy through a distributed anonymity algorithm that is Network Location and Data Anonymization technique with K- anonymity concept applied in a sensor network, before service providers gain access to the data. These procedures can provide a high amount of privacy, save service users from dealing with service providers.

### 3.1 Attacking model on WSN

In this paper we concerns WSN location privacy threat as a main topic in which an attacker can get an individual nodes location information with the help of the location system and they can identify the individual. For example, by using the location dependent system, attacker can track the position of every individual node in the domain. Frequently accessing this information would allow attacker to obtain the movements of an unknown user node. A more sophisticated attacker, with the help of local access to the sensor network ,he may attacks on the same network to get more precise location dependent information. Especially, the attacker could propose different types of attacks like Passive Attacks, Eavesdropping, Network Traffic analysis and Thread activities.

### 3.2 Network location and Data anonimization

In our explanation there are seven local sensor nodes, from A to G, and the required anonymity level is k = 5. Every node of this procedure will have a unique ID, but nodes within the same location will share the same location ID which hierarchy is statically configured during system installation. Coordination Leader(CL) election and network routing table setup uses a three-way handshake protocol. This operation starts with the top level root node, such as a base station or the location dependent server to select CLs for the higher level. This selection happens at every certain interval of time. When that interval of time occurs, each sensor node prepares and sends a message with its group identity, sensing area (domain), and the number of other nodes located in its remote sensing area to its neighbours as well as to CL. The selected CLs than recursively apply the same protocol, in order to find CLs for their lower levels up to leaders are elected for all levels of node hierarchy. After the initial broadcasting, all sensor nodes from A to F have found an sufficient number of objects.

In second state they are with cloaked area, where every sensor node captures its sensing area into the cloaked area that includes minimum k objects, in order to satisfy the k-anonymity privacy principles. For example peer list of main sensor node A having the information of adjacent three peers named by B, D, and E. The object of count as sensor nodes B, D, and E is 3, 1, and 2. We can assume that, there is some distance from main sensor node A to sensor nodes B, D, and E respectively. Since B has the high score, so we selected B. The total sum of the objects count in the given domain of A and B is six which is larger than the expected and required anonymity level k = 5, so we have to return the MBR of the remote sensing area of the n sensor nodes in S. for example node A and node B, as the node-aware cloaked area of A. The quality-aware anonimity algorithm the attackes the cloaked area computed by the resource-aware algorithm as an primary solution, and then refines it up to the cloaked area goes to the minimal possible area, which is still satisfying the k-anonymity privacy requirement, depends on the additional communication between all other peers. The K-anonymity quality-aware algorithm [8] specifies every domain node current minimal cloaked area by the input initial solution. We repeat this procedure until we produce the node sets at the highest level of the lattice precision structure or all the other item node sets at the current level are pruned.

 

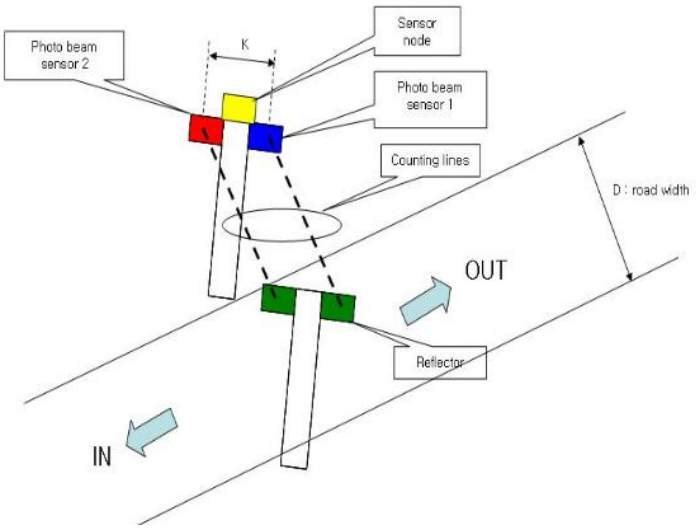


Fig.2. Deployed WSN Environment.

**Data Cloaking:** WSN Nodes employ two basic techniques in order to increase anonymity: To provide least spatial accuracy and to get the high precision to the count of subjects in the selected domain. In our hierarchical manner, high spatial accuracy, recall and precision can be achieved by omitting a domain of the less significant bit code information of the sender rnode ID. for that we are implemented two procedures are: i) Data Cloak ID, provide precise node data ii). Cloak Data, provide node precise ID. Our proposed domain wise data cloaking algorithm combines these two approaches. Every data node stores the desired anonymity level value k, which is preconfigured by the time of domain configuration. If the number of issues reaches or exceeds k the algorithm cloaks data and provides a precise data node ID , otherwise, it provides precise data with a cloaked ID.

## IV. EXPERIMENTS

Experiments of Network Location and Data Anonymization have been implemented in CGAL [9], a computation algometry library. In the first set of experiments, we compare the performance of the proposed cloaking method with the Hilbert cloaking method. In the simulations, n user locations are randomly placed in a1000×1000area.Performance of the two methods with respective to the level of K -anonymity where the number of users where n fixed at 1000 and K fixed at 10, respectively. The y-axis gives the size of the cloak as the percentage of the size of the area. Also shown in the figures are the error bars corresponding to the maximum and minimum cloak sizes. As can be observed in Figures 3, the LSH-based approach is significantly better than the Hilbert curve-based method . As K increases, the cloak size increases roughly linearly in both methods. With more users, it is expected that the cloak size decreases linearly. This trend is more prominent with the proposed LSH-based method.

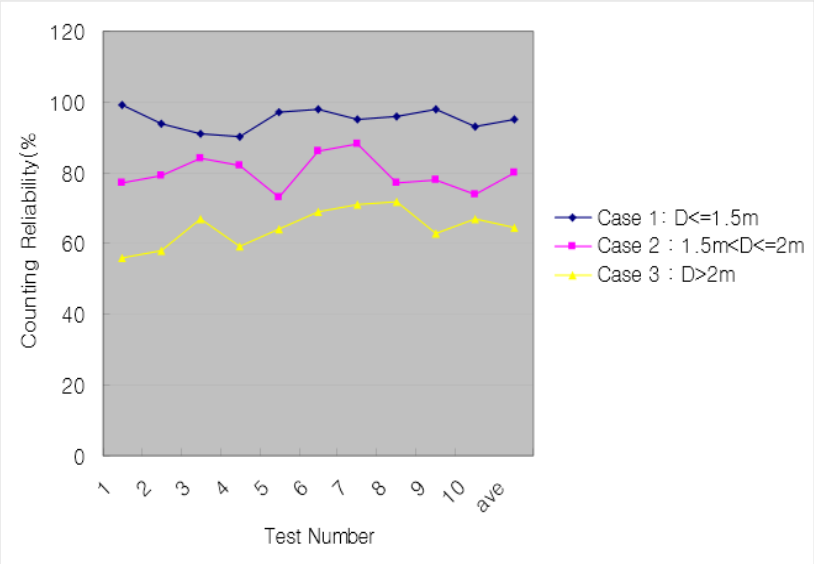


Fig.3. node counting Accuracy with NLDA.

## V. CONCLUSION

In this paper, we proposed a privacy policies to preserve the location monitoring system for wireless sensor networks. To avoid the problems in wireless sensor networks in this paper we introduced the Network Location and Data Anonymization technique with K- anonymity concept. This concept preserves the privacy of monitored person's sensitive information in wireless sensor networks. In order to minimize the computation and location monitoring cost we deployed spatial histogram approach to the network server nodes.

 

**REFERENCES**

[1] k-anonymity privacy protection using generalization and suppression,L.Sweeney,AchievingIJUFKS, vol. 10, no. 5, pp. 571–588, 2002.

[2] B.Gedik and L. Liu,"Protecting location privacy with person-alized k-anonymity: Architecture and algorithms," IEEE TMC,vol. 7, no. 1, pp. 1–18, 2008.

[3] M. F . Mokbel, C.-Y. Chow, and W. G. Aref, "The New Casper: Query procesing for location services without compromising pri-vacy ," in Proc. of VLDB, 2006.

[4] Rossi, M., Bozzoli, A., "Tracking and Counting Mo ving People," IEEE Proc. of Int. onf. Image Processing. 3, pp. 212-216, 1994.

[5] "PDA: Privacy-preserving data aggregation in wireless sensor networks, by W. He,X. Liu, H. Nguyen,K. Nahrstedt, and T. Abdelzaher," in Proc. of Infocom, 2007.

[6] Query privacy in wireless sensor networks by B. Carbunar, Y . Y u, W. Shi, M. Pearce, and V . Vasudevan, "in Proc. of SECON, 2007.

[7] ward, A.Sensor-driven Computing . PhD thesis, University of Cambridge, August 1998.

[8] Gabriel Ghinita. Private queries and trajectory anonymization: a dual perspective on location privacy. Trans. Data Privacy , 2:3–19, April 2009.

***Author Details:***

**Author 1:**

Mr. P.Jayasankar, M.Tech (CSE) from Acharya Nagarjuna University. I am presently working as Associate Test Architect in Alliance Global Services in Hyderabad. I am having 8 years of experience as a Test Lead. My interested subjects are Embedded Systems, Computer Networks, Network Security, Operating Systems and Computer Organization.

Mail Id:pandurusankar@yahoo.com

**Author 2:**

**Mr. B. Sunil Kumar** working as Assistant Professor in Department of Computer Science & Engineering in Jawaharlal Nehru Institute of Technology, I am having 3years and 6 months of Teaching Experience. My interested subjects are Web Technologies, Network Security, Web services, Mobile computing, cloud computing, Computer Networks, Operating System, Computer Organisation, Java, C, and C++.

Mail id: sunilkumar0060@gmail.com

**Author 3:**

**Dasari.Kiran Kumar** M.Tech from ANU Guntur, completed M.C.A from KU, Warangal,. I am presently working as Assistant Professor in Department of Computer Science Engineering in Vignana Bharathi Institute of Technology, Ghatkesar, Aushapur, Hyderabad. I am having 5years of Teaching Experience. My interested subjects are Software Engineering, Data mining, Web services, Web Technologies, Java, C, and C++.....

kiran_cgp@yahoo.com

**Author 4:**

**Mrs. T.P.Sarachandrika**, M.Tech (CSE) from Acharya Nagarjuna University. I am presently working as Assistant Professor in Department of Computer Science & Engineering in Sri Venkateswara College of Engineering - Tirupathi. I am having 5 years of teaching experience. My interested subjects are Operating Systems, Computer Organization, Software Engineering and Data Base Management Systems.

Mail Id: sarachandrika@gmail.com

 