Secured Location Monitoring System in Wireless Sensor Networks

Koteswara Rao Makkena[1], Ch. Ramesh Kumar[2]

[1]Pursuing M.Tech(CSE), Nalanda Institute of Engineering & Technology, Siddharth Nagar, Sattenapalli, Guntur., Affiliated to JNTUK, Kakinada, A.P., India.

[2]Asst. Professor, Department of Computer Science Engineering, Nalanda Institute of Engineering & Technology, Siddharth Nagar, Sattenapalli, Guntur., Affiliated to JNTUK, Kakinada, A.P., India.

***Abstract*— A wireless sensor network is deployed to monitor certain events and pinpoint their locations, the location information is intended only for legitimate users. However, an eavesdropper can monitor the traffic and deduce the approximate location of monitored objects in certain situations. This paper presents a secured location monitoring system in which we can monitor moving objects in wireless sensor networks while preserving their location privacy. The method consists of two main modules, in-network location anonymization and aggregate query processing over anonymized locations. In the first module, trusted wireless sensor nodes collaborate with each other to anonymize users' exact locations by a cloaked spatial region that satisfies a prespecified privacy requirement. On the other side, the aggregate query processing module collects and analyzes the cloaked spatial regions reported from the wireless sensor nodes to support aggregate and alarm queries over anonymized locations.**

***Keywords*— Wireless sensor network, privacy, monitoring system.**

I. INTRODUCTION

The emergence of the state-of-the-art devices and communication techniques in wireless sensor networks has resulted in many new applications for military and civilian purposes. Examples of these applications include surveillance and location monitoring systems. Such applications support wide variety of important functionalities that include. (1) Density queries, e.g., determine the number of moving objects within a specified region", (2) Safety control, e.g., send an alarm if the number of persons in a certain area exceeds a prespecified threshold", and (3) Resource management, e.g., turn of some building facilities if the number of people in a certain area is less than a certain threshold". Such location monitoring applications rely on deploying wireless sensor nodes that are able to communicate with a small wireless transmitter attached to human bodies to determine human's exact locations and identities.

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 [6]. 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 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.

Although location monitoring systems promise convenience and safety, with untrustworthy server, adversaries could abuse the personal location information to track people or reveal some sensitive information. Figure 1 gives an example of a privacy threat that can take place in location monitoring systems. Figure 1a depicts a floor plan of a certain building at time ti in which there are 11 sensor nodes installed in nine rooms R1 to R9 and two hallways C1 and C2. Each sensor node reports the exact location of each user within its monitoring area to a server. Figures 1b and 1c give the readings reported by the same sensor nodes at two consecutive time instances ti+1 and ti+2, respectively. If an adversary knows that Alice is in room R3 at time ti, then the adversary can know that Alice has left her room at time ti+1 and went to C2. Likewise, the adversary can reveal that Alice has left C2 at time ti+2 and went to R7. Such knowledge leakage may lead to several privacy threats. For example, tracking the personal behavior in a clinical building may reveal the personal medical record by knowing the particular clinic that the person has visited. Similarly, employers can use the location monitoring application to invade their employees' privacy by checking how long their employees are out of their cubes every day and where do they spend their time, e.g., chatting with other employees, in restrooms, or walking around [7,8].

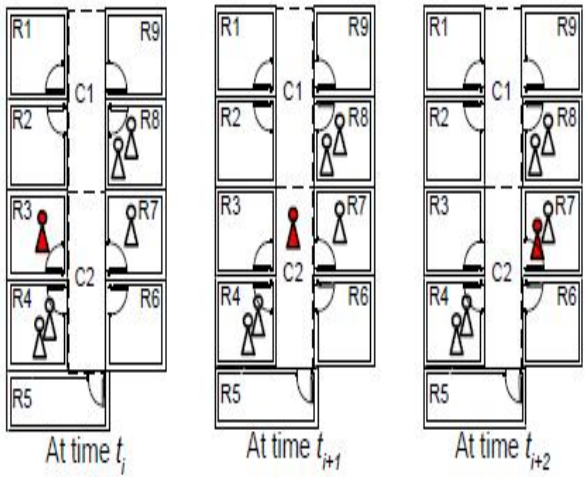

Figure 1: Privacy threats in surveillance systems

This paper presents the secured location monitoring system that aims to enable all sensor-based monitoring functionalities without sacrificing the privacy of tracked objects. The proposed system has two main modules, namely, in-network location anonymization and aggregate query processing over anonymized locations. The first module mainly aims to blur the exact user location within the monitoring area of each sensor node into a cloaked spatial region that contains at least k objects. If the number of users within the monitoring area of a certain sensor node is less than a prespecified privacy threshold k,that sensor node will exchange information with other sensor nodes to come up with a larger monitoring area that contains at least k objects. Figure 2 depicts the same example of Figure 1 when applying the anonymization module of proposed method with k = 3. At time ti, both the sensor nodes at R3 and R4 report the same region with number of objects = 3 while the sensor nodes at R7 and R8 report the same region with also number of objects = 3. Then, at time ti+1, an adversary would know that someone has entered C2. However, the adversary cannot pinpoint who is that person, instead the adversary can say that this person is one of the three persons that were in R3 and R4 at time ti. Thus, the areas and the count numbers reported from sensor nodes make all users k-anonymous, i.e., indistinguishable among k users (k = 3). Similarly, at time ti+2, an adversary cannot infer that Alice has entered R7. The second module of proposed method , i.e., aggregate query processing, aims to provide all monitoring functionalities (i.e., aggregate queries and alarm queries) based on the anonymized data received from Figure 2 instead of the actual data received from Figure 1.

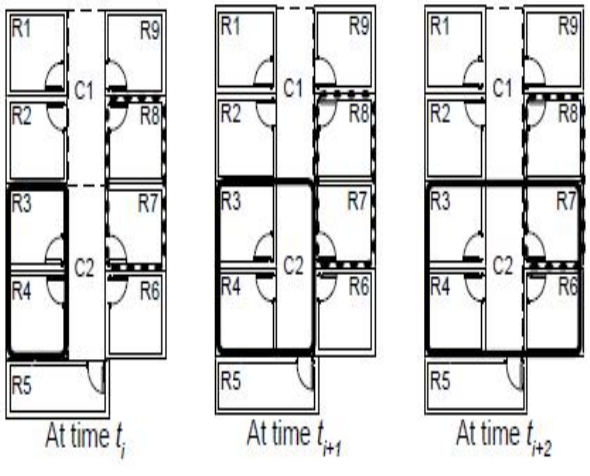

Figure 2: Anonymized locations in secured location monitoring system.

II. SYSTEM ARCHITECTURE OF THE PROPOSED SYSTEM

Figure 3 depicts the system architecture of proposed method, in which only the wireless sensor nodes are trusted. As has been mentioned in Section 1, proposed method consists of two main modules, in-network location anonymization and aggregate query processing over anonymized locations. In the location anonymization module, the wireless sensor nodes collaborate with each other to find their cloaked spatial regions, and then send the cloaked spatial region along with the number of objects within the region to a server via secure and anonymous communication. Proposed method can employ any existing anonymous and secure communication techniques designed for wireless sensor networks. On the other side, the aggregate query processing module is embedded inside the server to support aggregate query processing over anonymized locations. Proposed system administrators can change the privacy requirement, i.e., k-anonymity requirement, at anytime. Finally, system users can issue snapshot and continuous aggregate and alarm queries through the server terminals.

III. LOCATION ANONYMIZATION

The location anonymization module consists of two phases. (1) Initial anonymization phase. In this phase, sensor nodes with a non-zero object count broadcast a message containing their IDs, monitoring areas, and IDs of the detected objects. When the peers receive these messages, they rebroadcast them until all their neighboring sensor nodes have enough number of objects, i.e., at least k objects. Then, the cloaking sensor node calculates a score for each peer of the received messages. The score is defined as a ratio of the number of objects to the area of the minimum bounding rectangle covering the monitoring area of both the cloaking sensor node and the peer. Finally, the cloaking sensor node selects the peers with the highest score repeatedly until at least k objects are found. The cloaked spatial region is computed as the minimum bounding rectangle covering the monitoring area of the cloaking sensor node and the selected peers. The sensor node reports the cloaked spatial region with the number of objects within the region to the server. (2) Incremental maintenance phase. After the sensor node finds a cloaked spatial region, the sensor node registers itself with the selected peers. The sensor node will be notified by these peers whenever these peers detect any changes in their detected objects. If the sensor node does not have enough number of objects, the sensor node will enlist its peers for help to find more objects.

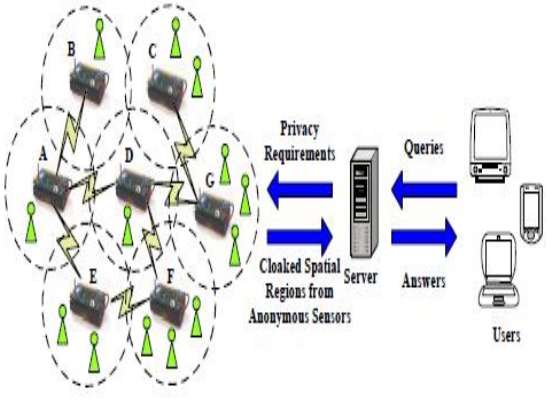

Figure 3: System architecture

IV. QUERY PROCESSING OVER ANONYMIZED LOCATIONS

The aggregate query processing module supports aggregate and alarm queries over anonymized locations without knowing users' exact locations. For an aggregate query, given a query region, the query processor returns the number of objects within the query region. For an alarm query, given a query region and a threshold, the query processor keeps track of the density of the query region, i.e., the number of objects within the query region divided by the query region area. The query processor notifies the querying user whenever the density is larger than the threshold. The main idea of the aggregate query processing module is to continuously maintain a spatio-temporal histogram to estimate the number of objects within each monitored area. The spatio-temporal histogram divides the system space into N disjointed equal-sized cells. We assume that the query processor is able to know the total number of objects M in the system. This can be achieved by installing wireless sensors at all entrances of the monitored building to count the number of objects entering and leaving the building. Initially, the query processor assumes that existing objects are evenly distributed in the system. Thus, the estimated number of objects located within each cell is b N1= M/N. Whenever the query processor receives a cloaked spatial region R along with the information about the number of objects RN within this region, the query processor refines the histogram by performing two key steps. (1) The query processor determines the difference diff between RN and b N of the cells overlapping with R. (2) The query processor updates the histogram by uniformly distributing RN (or diff) among the cells within (or outside) R.

V. CONCLUSION

This paper presents a secured location monitoring system in which we can monitor moving objects in wireless sensor networks while preserving their location privacy. The method consists of two main modules, in-network location anonymization and aggregate query processing over anonymized locations. In the first module, trusted wireless sensor nodes collaborate with each other to anonymize users' exact locations by a cloaked spatial region that satisfies a prespecified privacy requirement. On the other side, the aggregate query processing module collects and analyzes the cloaked spatial regions reported from the wireless sensor nodes to support aggregate and alarm queries over anonymized locations.

REFERENCES

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

[2] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, .The cricket location-support system,. in *Proc. of MobiCom*, 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=comcontent&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. James. Can't Hide Your Prying Eyes. Computerworld, 38:35{36, 2004. http://www.computerworld.com/securitytopics/security/privacy/story/0,10%801,90518,00.html.

[8] G. Kaupins and R. Minch. Legal and Ethical Implications of Employee Location Monitoring. In Proceedings of the Hawaii International Conference on System Sciences, 2005.

AUTHORS PROFILE

Koteswara Rao Makkena, Pursuing M.Tech(CSE) from Nalanda Institute of Engineering & Technology, Siddharth Nagar, Sattenapalli, Guntur., Affiliated to JNTUK, Kakinada, A.P., India. My research Interests are Mobile Computing.

Ch. Ramesh Kumar, working as Asst. Professor, Department of Computer Science Engineering at Nalanda Institute of Engineering & Technology, Siddharth Nagar, Sattenapalli, Guntur Affiliated to JNTUK, Kakinada, A.P., India. My research Interests are Mobile Computing,Data Mining.