ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

Resource Aware Location Monitoring Anonymization System For Wireless Sensor Networks

Bravim J. Jorewar [1] Dr.A. S. Alvi[2]

M.E. (I.T.) Scholar, Department of Information Technology, Prof. Ram Meghe Institute of Technology and Research Badnera, Amravati, Maharashtra, India[1]

Head Of Department, Department of Information Technology, Prof. Ram Meghe Institute of Technology and Research Badnera, Amravati, Maharashtra, India[2]

Abstract: Anonymzing wireless sensor networks allow users to access services from the server. In the network there can be a solitude threat of which users can view the content of the other users. Users can even modify copy or perhaps delete the information. 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 interaction and computational cost. To utilize the aggregate location information to provide location monitoring services, we use a spatial histogram approach that estimates the allocation of the monitored persons based on the assemble aggregate location information. Then the predictable distribution is used to allow 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 pledge the location privacy of the monitored persons.

Keywords: Wireless Sensor Network, Aggregate Location, Context privacy, Location System.

I. INTRODUCATION

Wireless sensor networks (WSN main purpose of the WSN is to supervise some physical phenomena (e.g., temperature, barometric pressure, light) inside an area of exploitation. Nodes are outfitted with radio transceiver, processing unit, battery and sensor(s). Nodes are inhibited in processing power and energy, whereas the base stations are not rigorously energy resources[1].The base station perform as gateways between the WSN and other networks such as Internet etc. The WSN is used in various applications like military, health and commercial. WSNs are becoming one of the building blocks of constant computing. They provide simple and despicable procedure for monitoring in the precise area. But WSN technology is an inappropriate use can appreciably breach privacy of humans. WSNs are frequently deployed to collect sensitive information. WSN can be used to monitor the movements of transfer in a city. Such a network can be used to verify position of people or vehicles. The sensor nodes such networks are deployed over a geographic area by aerial dispersion or other means. Each sensor node can only sense events within a very limited distance, called the sensing range. In addition, sensor nodes normally have moderately limited broadcast and reception capabilities so that sensing data have to be relayed via a multihop path to a far-away base station (BS), which is a data collection centre with adequately powerful processing capabilities and assets. With identity sensors, the system can pinpoint the exact location of each monitored person[5][3]. Regrettably, monitoring personal locations with a potentially un-trusted system poses privacy intimidation to the monitored individuals, because an opponent could abuse the location in succession gathered by the system to infer personal sensitive information. For the location monitoring system using identity sensors, the sensor nodes report the exact position in turn of the monitored persons to the server; thus using identity sensors instantly poses a major privacy breach. Even though the counting sensors by nature provide aggregate location information, they would also pose privacy breaches[9].

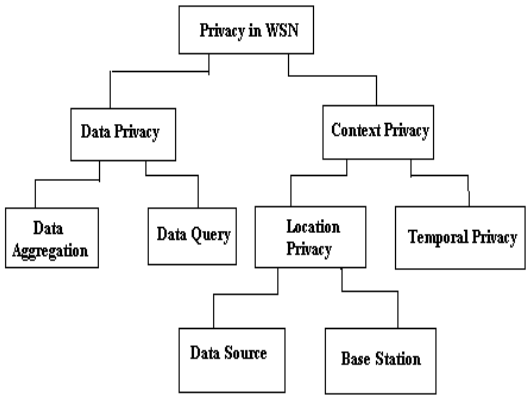

Fig1:Privacy Preserving protections in WSNs

II. MOTIVATION

The advance in wireless sensor techniques has resulted in many new applications for military and/or civilian purposes. Many cases of these applications rely on the in sequence of personal locations, for example, inspection and location systems. These location-dependent systems are comprehend by using either identity sensors or

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

counting sensors. Photoelectric sensors and thermal sensors are arrange place to report the number of persons located in their sensing areas to a server. Regrettably, monitoring personal locations with a potentially entrusted system poses solitude threats to the monitored individuals, because an rival could violence the location information gathered by the system to conjecture personal sensitive information[8]. For the location monitoring system using identity sensors, the sensor nodes details the exact location information of the monitored persons to the server; thus using identity sensors instantly poses a major privacy contravention [3][5].

III. RELATED WORK

A. *K-ANONYMITY PRINCIPLE*

While anonymity is define as "being unknown "or "of unknown authorship", information privacy researchers construe it in a stronger sense. "anonymity is the state of being not identifiable within a set of subjects, the anonymity set". we consider a subject as k-anonymous with respect to position information, if and only if the position information presented is indistinguishable from the position information of at least k 1 other subjects. Privacy preservation we have generally found that as long as location information is aggregated over a group of individuals, publish does not violate privacy[2][13]. *k*-anonymity provides a suitable way of simplify. This concept is user is *k* anonymous if and only if it is unfeasible to tell apart simplify at least k users in its be familiar with information . The key step in making position information in anonymous is to simplification. The K-anonymity principle is :a query is considered personal, if the possibility of identifying the querying user does not exceed 1/K, where K is a user-specified anonymity obligation. K anonymity condition is "each leave go of data must be such that every combination of values of quasi-identifiers can be imprecisely matched to at least k-1 individuals[4][6]" Anonymity level is set by supervisor of a system to provide security for mobile users in a conviction zone. The moving objects are shown by green color. What basically happens in a system is a user is asking some query concerning any user in a zone to a server. Server passes this query to a sensor nodes present in trusted zone. Then sensor node from one area will swap message with the other and report an aggregate location to the server and then server will send the answer to the user[8][10].

B. *LOCATION ANONYMIZATION ALGORITHM*

It recommend resource-aware anonymization algorithms in wireless sensor networks .In this algorithm concept of *k* anonymity solitude requirement is used. The resource-aware Algorithm aims to minimize interaction and computational cost, the accuracy of the aggregate locations by minimizing their monitored areas [10][11].

1) *THE RESOURCE-AWARE ALGORITHM:*

It designate that the sensor nodes can communicate directly with each other. This algorithm consists of three steps; transmit step, shrouded area step, cloaked area step. Algorithm outlines the resource-aware location anonymization algorithm [4][10].

a) THE TRANSMIT STEP:

It is to guarantee that each sensor node knows an sufficient number of objects to calculate a shrouded area. To reduce communication cost, this step relies on a heuristic that a sensor node only forwards its received messages to its neighbors when some of them have not yet found an enough number of objects. In this step, after each node m initializes an vacant list Peer List, m sends a with its identity m.ID, sensing area m.Area, and the number of objects located in its sensing area m.count, to its neighbors. When m receives a message from a peer p, m stores the message in its PeerList. Whenever m finds an plenty number of objects, m sends a notification message to its neighbors. If m has not received the notification message, some neighbor has not found an plenty number of objects, therefore m forwards the received message to its neighbors[12][13].

b)THE SHROUDED AREA STEP:

It is that each node blurs its sensing area into a shrouded area that includes at least k-objects to satisfy the k-anonymity Solitude requirement. To minimize computational cost, this step uses a ravenous approach to find a shrouded area based on the information stored in Peer List. For each node initializes in its Peer List. It includes at least k objects and has an area as small as possible. Finally, m determines the shrouded area that is a minimum bounding rectangle (MBR) that covers the sensing area of the nodes, and the total number of objects. An MBR is a rectangle with the least area that completely contains all desired regions.

c)THE VALIDATION STEP:

It is to keep away from reporting aggregate locations with a relationship to server. Each node preserve a list to hoard the aggregate.

IV. SYSTEM MODEL

System Architecture consists of user, server and trusted zone. There are sensor nodes and mobile users in a trusted zone .Anonymity level is set by administrator of a system to provide safety for mobile users in a trusted zone. The moving objects are shown by green color. What basically happens in a system is a user is asking some query regarding any user in a zone to a server. Server passes this query to a sensor nodes present in confidence zone. Then sensor node from one area will exchange message with the other and report an aggregate location to the server and then server will send the answer to the user[1][7].

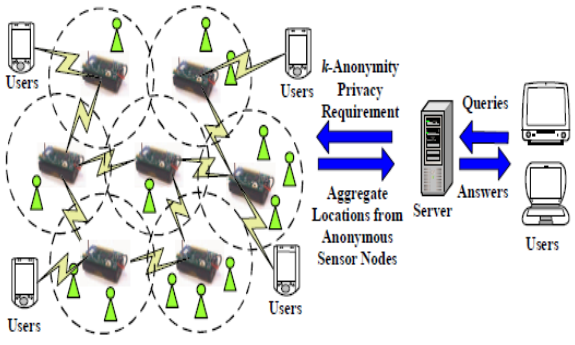

Fig 2: Architecture of system

A. *SENSOR NODE:*

There are a variety of sensor nodes present in a trusted zone. The job of Sensor nodes is to compute moving objects in its own area. Sensor nodes are unknown in nature. Sensor nodes communicate with the other sensor nodes to form a peer list by broadcasting a message. After a peer list sensor nodes forms a cloaked area in which there should be k no of objects present. The shroud area is the imprecise area which can't b seen by other sensor nodes. That cloaked area is the final aggregate location which is provided to a user through a server.

B. SERVER :

Server can be called as central node as every sensor node is associated to it. Server keeps information about all sensor nodes. Server can be called as communication medium between user and trusted zone i.e. sensor nodes. User first sends a query to a server and then server go beyond it to sensor nodes.

C. TRUSTED ZONE:

Trusted zone consist of several nodes as talk about earlier. This zone is called as trusted because the anonymous sensor nodes are present in it. Anonymous nature of sensor nodes helps hiding from other senor nodes.

V. CONCLUSION

In our system, sensor nodes execute our location anonymization algorithms to give k-anonymous aggregate locations, in which each aggregate position is a cloaked area A with the number of observe objects, N, located in A, where $N \geq k$, for the system. The resource-aware algorithm aims to minimize interaction and computational cost. To provide location monitoring services based on the aggregate location information. The results show that our system provides high quality location monitoring services.

ACKNOWLEDGMENT

I am privileged to work with my Guide, Dr. A.S. Alvi. I will also like to thank him for his direction and support during this thesis work. I will like to express my delight to whole staff for their mutual effort and technical support. Finally, I will like to thank to my whole family for their invaluable support and motivation during this entire period

REFERENCES

[1] Chi-Yin Chow, Student Member, IEEE, Mohamed F. Mokbel, Member, IEEE,and Tian He, Member, "Privacy- Preserving Location Monitoring System for Wireless Sensor Networks" IEEE transactions on mobile computing, vol. 10, no. 1, jan 2011.

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacy grid". in Proc. of WWW, 2008.

[3] Gayathri M ,Bharathi M ,"A K-Anonymity Privacy-Preserving Location Monitoring System for Wireless Sensor Networks with Nymble Secure System" International Journal of Computer & Organization Trends –Volume2Issue2- 2012.

[4] Giri M. S, Prof. Chirchi V. R," Survey On Location Anonymization Algorithms For Wsn" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 8, August – 2013.

[5] M.X.Aquien, T. Sudarson Rama Perumal, G.Kharmega Sundararaj" Node Distribution in Wireless Sensor Networks Using Component Based Localization Algorithm" International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 2.

[6] Zhenqiang Gong,Guang-Zhong Sun,Xing Xie,"Protecting Privacy in Location-based Services Using K-anonymity without Cloaked Region" Eleventh International Conference on Mobile Data Management.

[7] Shiv Sutar, Manjiri Pathak , Prerana Sonawane, Deepali Ugale,"Privacy Preservation by Anonymization and Location Monitoring System for WSN" (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.104-108.

[8] Sheng Zhong, Li (Erran) Li, Yanbin Grace Liu, Yang Richard Yang," Privacy-Preserving Location-based Services forMobile Users in Wireless Networks"

[9] D.Gayathri, Abdul Vahed," Anonymization Mechanism for Privacy-Preserving Location Monitoring System in WSN" (IJCTT) – volume 4 Issue 8– August 2013.

[10] Pandurang Kamat, Yanyong Zhang, Wade Trappe, Celal Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing".

[11] Gabriel Ghinita, Panos Kalnis, Spiros Skiadopoulos "Priv´e: Anonymous Location-Based Queries in Distributed Mobile Systems" WWW 2007 / Track: Pervasive Web and Mobility May 8-12, 2007. Banff, Alberta, Canada.

[12] Nikhil Kumar Sanghvi "EXPLORING SECURED LOCATION DATA FOR PRESERVING IN SCANNING SYSTEM" International Journal of Advanced Computer and Mathematical Sciences ISSN 2230-9624. Vol 3, Issue 3, 2012, pp 343-347http://bipublication.com

[13] Claudio Bettini, Sergio Mascetti,X. Sean Wang "Anonymity in Location-based Services: Towards a General Framework "

BIOGRAPHIES

Bravim J. Jorewar is student of second year M.E. (Information Technology) at Prof. Ram Meghe Institute of Technology and Research Bandera, Amravati – Sant Gadge Baba Amravati University, Amravati, Maharashtra, India

Dr. A. S. Alvi is Head Of Department, Department (Information Technology) at Prof. Ram Meghe Institute of Technology and Research Bandera, Amravati. He has completed his PhD in CSE. - Sant Gadge Baba Amravati University, Amravati, Maharashtra, India