International. Journal of Engineering Research and Application www.ijera.com ISSN : 2248-9622, Vol. 6, Issue 9, (Part -5) Sepamber 2016, pp.93-98

RESEARCH ARTICLE OPEN ACCESS

WSN: A Protected Object Location Monitoring

Dr.S Krishna Mohan Rao[1], Pragyan Paramita Mahala[2], Manmath Nath Dash[3]
[1,3]*Associate Professor, Department of Computer Science Engineering, Gandhi Institute For Technology (GIFT), Bhubaneswar*
[2]*Assistant Professor, Department of Computer Science Engineering, Gandhi Engineering College, Bhubaneswa*

ABSTRACT
The Connectionless Sensor Networks is nothing but wireless Sensor Network (WSNs).Much of the existingworkonwireless sensor networks has focused on addressing the power and computational resource constraints of WSNs by the design of specificrouting,MAC,andcross-layerprotocols.Recently,there have been heightened privacyconcerns over the datacollectedby and transmitted through WSNs.The wireless stransmission required by a WSN, and the self-organizing nature of its architecture, makes privacy protection for WSNs an especially challenging problem.LocalityObservingMethodsareusedtodetecthumanactivitiesand provide monitoring services. We consider an aggregate Locality Observing Method where wireless sensor nodes are counting sensorsthatareonlycapablofdetectingthenumberofobjectswithintheirsensingareas.Actuallythepersonallocationisbeing monitored by a third party (untrusted server), are vulnerable to privacy threats. The wireless sensor networks allowuserstoaccessservicesprivatelybyusingaseriesofrouterstohidetheclient'sIPaddressfromtheserver.Weproposea privacypreservingLocality Observing Method for wireless sensor networks. In our system, we design two in-network location anonymization algorithms, namely, Cloaked Area Determination Algorithm and quality enhancedhistogramalgorithmthatwillhelpthesystemtoenableandprovidehighqualitylocationmonitoringservicesfor system users, while preserving personal location privacy. The Cloaked Area determination algorithm aims to minimize communication and computational cost, A quality enhanced histogramapproach is used 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 rangequeries
Keywords : WirelessSensorNetworks,LocalityObservingMethod,Aggregate Query Processing, Spatial Histogram, Anonymous Blacklisting, Privacy, Misbehaving Users LocationPrivacy

I. INTRODUCTION

Awirelesssensornetwork(WSN)isawireless networkconsisting of spatially distributed autonomous devices that use sensors to monitorphysicalorenvironmentalconditions.Thesea utonomous devices, or nodes, combine with routers and a gateway to create a typical WSN system. The distributed measurement nodes communicate wirelessly to a central gateway, which provides a connection to the wired world where you can collect, process, analyze, and present your measurement data. To extenddistance and reliability in a wireless sensor network, you can use routers togainanadditionalcommunicationlinkbetweenendn odesand thegateway.
NationalInstrumentsWirelessSensorNetworksofferr eliable,lowpowermeasurementnodesthatoperateforu ptothreeyears on 4 AA batteries and can be deployed for long-term, remote operation. The NI WSN protocol based on IEEE 802.15.4 and ZigBeetechnologyprovidesalowpowercommunicati onstandardthat offers mesh routing capabilities to extend network distance and reliability. The wirelessprotocolyouselectforyournetwork depends on your application requirements. To learn more aboutotherwirelesstechnologiesforyourapplication,re adthe"Selecting the Right Wireless Technology" whitepaper.

Fig.1:WirelessSensorNetworkArchitecture

In the present world, use of internet is increasing increasingly. User data and other vital dataflowsthroughtheinternet.Thisdataispronetobemisusedbyexternalentities.Eventhoughthereare several policies to prevent data misuse, thesearen'tfoolproof.Theproposedsystemaimstohidedatathatisvitaltopreservetheprivacyofanyuser.Systemproposestousekanonymityconcepttoachievethistask.Systemproposestouseasensornodenetworktotracethepeople.Thelocationoftheseuserswillbemonitored but this vital data will be prevented from being available and misused by external entities.

A. Wireless SensorNetworks

A large collection of densely deployed, spatially distributed, auto nomous devices (ornodes) that communicate via wireless and cooperativelymonitorphysicalorenvironmentalconditions.The sensornodes such networks are deployed overageographicareabyaerialscatteringorothermeans.Eachsensornodecanonlydetecteventswithinaverylimiteddistance,calledthesensingrange.Inaddition,sensornodesnormallyhavefairlylimitedtransmissionandreceptioncapabilitiessothatsensingdatahavetoberelayedviaamultihoppathtoadistantBaseStation(BS),whichisadatacollectioncenterwithsufficientlypowerfulprocessingcapabilitiesandresources.

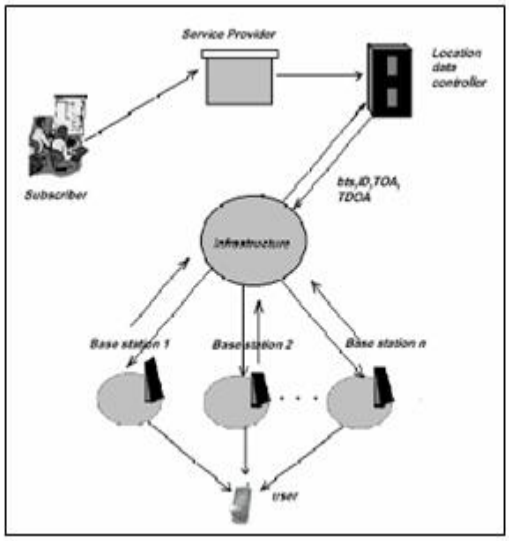


Fig. 2: Wireless Sensor Network

B. Locality ObservingMethod

Locality Observing Methods are used to detect human activities and provide monitoring services. We consider an aggregate Locality Observing Method where wireless sensor nodes are counting sensors that are only capable of detecting the number of objects within their sensing areas.

C. LocationPrivacy

Location privacy is a particular type of information privacy. It is defined as the ability to prevent other parties from learning one's current or past location. Usually position is computed and maintainedbyanexternalsource,suchastheunderlying network.

Inamobilecommunicationsnetwork,thisisnecessaryinorderto route calls to and from subscribers within thenetwork.

I. ExistingSystem

Existing Locality Observing Methods. In an identity-sensor Locality Observing Method, since each sensor node reports the exactlocationinformationofeachmonitoredobjecttotheserver, the adversary can pinpoint each object's exact location. On the otherhand,inacounting-sensorLocalityObservingMethod,each sensornodereportsthenumberofobjectsinitssensingareatothe server. The adversary can map the monitored areas of thesensor nodestothesystemlayout.Iftheobjectcountofamonitoredarea is very small or equal toone.

You can use several network topologies to coordinate the WSN gateway, end nodes, and router nodes. Router nodes are similar to end nodes in that they can acquire measurement data, butyou also can use them to pass along measurement data from other nodes. The first, and most basic, is the startopology,inwhicheachnodemaintainsasingle,directcommunicationpathwiththegateway.Thistopology issimplebutrestrictstheoveralldistance that your network can achieve.

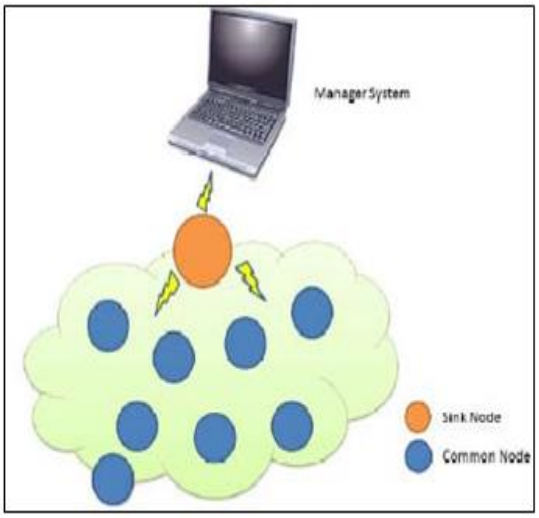


Fig. 3: Network Topologies

a. PROPOSED SYSTEM

Theproposedsystemaimstopreserveprivacyofindividualswhile releasing a part of their information, regarding their location. System relies on k anonymity concept within which a person cannot be distinguished among k-persons.

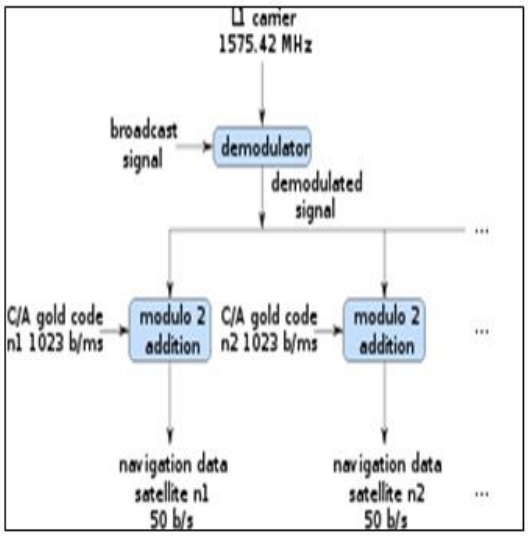


Fig. 4: GeoLocation System Architecture

Systemmakesuseoftwoinnetworkanonymizationalgorithms,cloakedareadeterminationalgorithm.SystemalsousesaQualityEnhancinghistogramapproachtoenhancethelocationmonitoringquality.Theexternalagency,needinglocationdataofanyparticular individual,sendsaquerytotheserver.Theserver,inturntransfers this query to the WSN, comprising all the sensor nodes. Sensor nodes, on receiving this query, work independently, to obtain theaggregatelocationinformationofagroupofkpersons.Each sensor node obtains aggregate information ofkpersonsinitsareaandfinallyreportsthisinformation totheserver.Theserver finally tries to enhance the quality of location monitoring by using a Quality Enhancing histogram and sends the aggregate information to the external agency. So, even the serverhasnoaccesstotheexactconcernedindividuallocationinformation,asitreceivesaggregatelocationofkpersonsfromeachsensornode.Systemaimsthispurposesince`theserverisuntrustedandcanbe misused by several attacks, some of them being eavesdropping, hacking, sending malicious codes, etc. [1] We design two in- network location anonymization algorithms, namely,cloaked area determination algorithm and quality-aware algorithm that will help the system to enable and provide high-quality location monitoring services for system users, while preserving personal location privacy. Cloaked Area Determination Algorithm.This algorithm is executed by all the sensor nodes, on receiving query from the server, for particular individuallocationinformation.Thisalgorithmaimstominimizethecommunication and the computation cost of the system. This algorithm follows the followingsteps:

A. Helps Each Sensor Node to Find Adequate no. of Persons in its Area

Inoursystem,fewsensornodesareconnectedtoeachotherandcandirectlycommunicatewitheachother,whilefewcannot.Sensor nodes who can directly communicate with each otherarecalledneighbors.Duringthereportingperiod,eachsensornodetriestodetermineadequateno.ofpersonsinitsarea.Ondetermining,each sensor nodes sends a notification to its neighbours. Notification comprisessensornodename,itsareaandtheno.ofpersonsinitsarea.Ifsomenodesareunabletodetermineadequateno.ofpersonsintheirareas,theycannotsendthisnotificationtotheirneighbours.So,tohelpthemfindadequateno.ofpersonsintheirareas,their neighbouring sensor nodes forward all the notifications they have received, to these sensor nodes. However, this notification forwarding procedure is followed only when sensor nodes are unable to determine adequate no. of persons in their areas. This approach helps to minimize the communication cost.

1. Demodulation and Decoding

- Sinceallofthesatellitesignalsaremodulatedontothesame L1 carrier frequency, there is a need to separate the signals after demodulation. Demodulating and Decoding of GPS Satellite Signals takes place using the Goldcodes.
- This is done by assigning each satellite a unique binary sequence knownasa Goldcode. Thesignalsaredecoded,after demodulation,usingadditionoftheGoldcodescorresponding to the satellites monitored by thereceiver.

Each SensorNodetoBluritsSensingAreainto a CloakedAreaWhen this step begins, each sensor node has found outadequate no. of persons in their areas. To reduce the computational cost, algorithm follows a greedy approach. Using this approach, each sensor node is able to determine their cloaked areas, containing at least k persons. Each sensor nodes has received adequate notificationsfromtheirneighbours.Now,ascorevalueiscomputed byeverysensornode,forallthenotificationsithasreceived.Letusconsider3nodes:A,BandC.ForsensornodeA, Scorevalue is computed by the following formula:Score=No.ofpersonsunder(BorC)/Euclidiandistancebetween A and (BorC)Euclidiandistanceisthedistancebetweenanytwosensornodes.ProposedsystemassumestheEuclidiandistancebetweenallthe sensor nodes.When all the score values are obtained (i.e. for A & Band A&C), the highest valueisconsidered. SupposeifA& B has the highest value. Then, we design a Minimum Bounding Rectangle (MBR), to compute the

cloaked area of sensor node A.
In this case, the MBR will contain the areas under sensor nodes A and B. This obtained MBR is nothing but the cloaked area of sensor node A. Similarly, other sensor nodes B and C, compute their cloaked areas.

B. Selecting CloakingSet

Itmayfirstappearthatwecandeterminethecloakingset,denotedasS,byfindingthesetofuserswhohavefootprintsclosesttothestartingpointoftheserviceuser.Thissimplesolutionminimizes the size of the first cloaking box. However, as the service user moves, the users in S may not have footprints that are close to her current position. As a result, the size of the cloaking boxes may become larger and larger, making it difficult to guarantee the quality of LBS. Thus, when selecting the cloaking set, we should consider its affect on the cloaking of not only the user'sfirstbutalllocationupdatesintheLBS.Butthechallengeisthat the service user's route is not predetermined, and thus the LDS cannot figure out whose footprints will be closer to the service user during her travel. To address this challenge, our ideaistofindthoseuserswhohavevisitedmostplacesintheserviceuser's travel bound B and use them to create the cloaking set. As these users have footprints spanning the entire region B, it will help generate a PPT with a fineresolution.

WesayauserislpopularwithinB,ifshehasfootprintsinevery cell at level l that overlaps with B. According to the pyramid structure, cells at level with a larger l have a finer granularity. This implies that given an l-popular user, the larger the value of l is, the more popular the user is. Figure 2 shows an example in which a network domain is partitioned intoa4levelpyramid(Thereare1,4,16,64cellsateachlevelrespectivelyfromtoptobottom).Italsoshowsatravelboundthefootprintsinsideit.Thefootprintsindifferentcolorsbelongtodifferentusers.u1, u2, and u3 are three 2-popular users within B because theyhavefootprintsinthetwocellsatlevel2ofthepyramidwhichoverlap with B; u2, u3 are two 3-popular users within B since they have footprints in all four cells at level 3 that overlap with B; only u3 is 4-popular since she is the only one who has footprints in all the sixteen cells at level 4 that overlap withB.
Cloaking Area determination algorithms

Algorithm 1 SelectCloakingSet($P(R)$, B)

1. $U \leftarrow \emptyset$ {U keeps the cloaking set}
2. $l \leftarrow h$
3. **while** $U \subset S(B)$ **and** $P_U(B) < P(R)$ **do**
4. {Get cells at level l overlapping with B}
5. $C_l' \leftarrow Overlap(C_l, B)$
6. {Join user tables of C_l' by column uid}
7. $T \leftarrow Join(C_l', uid)$
8. $U \leftarrow S_l \leftarrow T.uid$
9. $l \leftarrow l - 1$
10. **end while**
11. return U

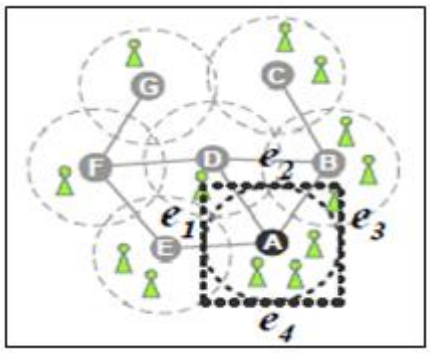
1. Computing CloakingBoxes

During a service session, the service user updates a time-series sequence of locations. For each location update p, the LDS computes a cloaking box b using the footprints of users in the cloakingset U. We develop a heuristic algorithm which computes the cloaking box bas small as possible, and ensures that PU(b)≥ P(R).ThepseudocodeisgiveninAlgorithm2.Givenalocation update p, the LDS first initializes the cloaking box b to p which is the smallest cloaking box only containing the service user herself.

Algorithm 2 Cloak(p, $P(R)$, U)

1. $F \leftarrow \emptyset$
2. $l \leftarrow$ the level where U is determined
3. $b \leftarrow p$
4. $b' \leftarrow$ the cell in C_l that contains p
5. **while** $P_U(b) < P(R)$ **do**
6. **for all** $u \in U$ **do**
7. $F_u \leftarrow$ the footprints of u in $b' \quad b$
8. $f_u \leftarrow$ the closest footprint to p in F_u
9. $F \leftarrow F + \{f_u\}$
10. **end for**
11. $b \leftarrow MBB(F)$
12. **if** b contains all footprints of U in b' **then**
13. {get cells at bottom level adjacent to b'}
14. $C' \leftarrow Adjacent(b', h)$
15. {merging the cells in C' with b'}
16. $b' \leftarrow b' \bigcup C'$
17. **end if**
18. **end while**
19. return b

TheLDSalsoinitializesasearchingboxb'tothecellthatcontains p at level l where the cloaking set U is selected in Algorithm 1, since it contains footprints of all users in the cloaking set.Then, for each user in U, the LD Sgetstheset ofherfootprintsFuwhich are inside b' but outside b, and in Fu the LDS finds the closest one to p (line 7-8). Next, the LDScollects.



Quality Advanced HistogramAlgorithm

InheproposedsystemQualityEnhancinghistogram[1]providesapproximatelocationmonitoring. QualityEnhancinghistogramisembeddedinsideservertoestimatethedistributionofthemonitoredobjectsbasedontheaggregatelocationswhicharereportedfrom sensor nodes. Quality Enhancing histogram is represented by a two dimensional array that represents a grid structure G of NR rows and NC columns; hence, the system space is divided into NR×NC disjoint equal sized grid cells. In each grid cell G(i; j), wemaintainafloat value that actsas` anestimatorH[i;j](1≤i

≤ NC,1 ≤ j ≤NR) of the number of objects within its area. In the proposed system we assume that the system has theability toknow thetotal number of moving objects Minthe system [8], [9].Initially,weassumethattheobjectsareevenlydistributedinthe system, so the estimated number of objects within each gridcell is H [i; j] = M/(NR ×NC). R stores set of aggregate locations reported from thesensornodes,givenasainputtothehistogram. Rcontainsacloaked area, R.Area,foreachaggregatelocation

R. and R.N is the number of monitored objects within R.Area. Initially, the aggregate locations in R are grouped into the same partition P = {R1,R2,……R|P |} if their cloaked areas are not overlapping with each other, which means that for every pair of aggregate locations Ri and Rj in P, Ri.Area ∩ Rj.Area=Φ. Then, foreachpartitionP,weupdateitsentiresetofaggregatelocationstotheQualityEnhancinghistogramandatthesametime,foreach aggregatelocationRinP,werecordtheestimationerror, whichis the difference between the sum of the estimatorswithinR.Area,R.N^,andR.N,andthenR:Nisuniformlydistributedamongtheestimatorswithin R. Area;hence,eachestimatorwithinR.Areais settoR.Ndividedbythetotalnumberofgridcellswithin R.Area. After processing all the aggregate locations in P, we sum up the estimationerrorofeachaggregatelocationinP.Thusthe estimator in the histogram is updated as shown in thealgorithm.

2. Quality Enhancing Histogram Algorithm[10]

1. Function HISTOGRAM(AggregateLocationSet R) 2: for each aggregate location r € R do
3: if there is an existing partition P={r…..r|P|}such that r.Area∩
r
Rk:Area = ; for every Rk.Area ={ } for every rk € P then
4. Add R toP
5. else
6. Create a new partition for R
7. End if
8. End for
9. each partition Pdo
10. for each aggregate location Rk € Pdo
11. 11.
12. 12.
13. for every cell g(i,j) € Rk.Area

$$\mathcal{H}[i,j] \leftarrow \frac{R_k.N}{\text{No. of cells within } R_k.Area}$$

14. End for
15. $P.Area \leftarrow R_1.Area \cup \cdots \cup R_{|P|}.Area$
16. for every cell g(i,j) € p.area

$$\mathcal{H}[i,j] = \mathcal{H}[i,j] + \frac{\sum_{R_k \in P} R_k.\bar{N} - R_k.N}{\text{No. of cells outside } P.Area}$$

17. end for

II. CONCLUSION

Thus, the proposed system aims to provide Secured Sheltered Locality Observing Method using WSN. Location monitoring is done using in-network location anonymisaton algorithms, namelyCloaked Area Determination Algorithm & Quality Aware Algorithm.Individual privacy will be preservedusingkanonymityprinciple.Qualityoflocation–monitoringwillbeenhancedusing Quality Enhancing Histogram approach. This system will be evaluated using simulated experiments. This approach will help thesystemt opreservelocation privacyofconcernedindividuals and at the same time, their location information released will be fruitful to the external agency. We have completed literature survey, Analysis, Design phases for developing ourproject.

REFEENCES

[1] TrafSysInc.,"PeopleCountingSystems",[Online]Available:http://www.trafsys.com/products/people-counters/thermal- sensor.aspx,2009.

[2] M. Gruteser, G. Schelle, A. Jain, R. Han, D. Grunwald, "Privacy-Aware Location Sensor Networks", Proc. Ninth Conf. Hot Topics in Operating Systems (HotOS),2003.

[3] G. Kaupins, R. Minch,"Legal and Ethical Implications of Employee Location Monitoring", Proc. 38th Ann. Hawaii Int'l

Conf. System Sciences (HICSS),2005.
[4] LocationPrivacyProtectionActof2001,[Online]Available: http://www.techlawjournal.com/cong107/privacy/location/ s1164is.asp,2010.
[5] Title 47 United States Code Section 222 (h) (2), [Online] Available: http:// frwebgate.access.gpo.gov/cgi-bin/getdoc. cgi?dbname=browse_usc&docid= Cite:+47USC222, 2009.
[6] D. Culler, M.S. Deborah Estrin,"Overview of Sensor Networks", Computer, Vol. 37, No. 8, pp. 41-49, Aug. 2004.
[7] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, J.D. Tygar, "SPINS: Security Protocols for Sensor Networks", Proc. ACM MobiCom,2001.
[8] J. Kong, X. Hong,"ANODR: Anonymous on Demand Routingwith Untraceable Routes for Mobile Ad-Hoc Networks", Proc. ACM MobiHoc,2003.
[9] P.Kamat,Y.Zhang, W.Trappe,C.Ozturk,"EnhancingSource-Location Privacy in Sensor Network Routing", Proc. 25th IEEEInt'lConf.DistributedComputingSystems(ICDCS), 2005.
[10] S. Guo, T. He, M.F. Mokbel, J.A. Stankovic, T.F. Abdelzaher," On Accurateand Efficient Statistica Counting in Sensor-Based Surveillance Systems", Proc. Fifth IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS), 2008.
[11] K. Bohrer, S. Levy, X. Liu, E. Schonberg,"Individualized Privacy Policy Based Access Control", Proc. SixthInt'l Conf. Electronic Commerce Research (ICECR), 2003.
[12] E. Snekkenes,"Concepts for Personal Location Privacy Policies", Proc. Third ACM Conf. Electronic Commerce (EC), 2001.
[13] L. Sweeney,"Achieving k-Anonymity Privacy Protection Using Generalization and Suppression", Int'lJ.Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, No. 5, pp. 571-588, 2002.
[14] H. Kido, Y. Yanagisawa, T. Satoh,"An Anonymous Communication Technique Using Dummies for Location-BasedServices",Proc.Int'lConf.PervasiveServices(ICPS), 2005.
[15] A.Harter,A.Hopper,P.Steggles,A.Ward,P.Webster,"The Anatomy of a Context-Aware Application", Proc. ACM MobiCom,1999.
[16] N.B. Priyantha, A. Chakraborty, H. Balakrishnan,"The Cricket Location-Support System", Proc. ACMMobiCom, 2000.
[17] B. Son, S. Shin, J. Kim, Y. Her,"Implementation of the Real-Time People Counting System Using Wireless SensorNetworks",Int'lJ.MultimediaandUbiquitousEng.,Vol.2, No. 2, pp. 63-80,2007.