ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Multihop Privacy Aware Data Aggregation in Mobile Sensing

Asmita Abhyankar, Prof.D.N.Rewadkar

M.E, Department of Computer Engineering, R. M. D. Sinhgad School of Engineering, Pune, India

H.O.D, Department of Computer Engineering, R. M. D. Sinhgad School of Engineering, Pune, India

ABSTRACT:Mobile phones specially smart phones are gettingmore and more importance in day to day life. More of thesemobile phones are now facilitated with number of applicationsthat are using sensors. With the help of large no. of individualparticipants, aggregation which is computed from data is reallyuseful and helps to predict the statistics of result. Aggregationguarantees more privacy of the data from individual participants.This paper provides a solution for preserving the individualparticipants privacy by using aggregate function like Sum, Min.Calculation of Sum aggregation is done without releasing theparticipants information. Min aggregation is calculated using Sum aggregation. Min aggregation is nothing but minimumvalue of data. In this paper, a multi-hop network is consideredwhere,there is a main aggregator at the highest level and mobilenodes are considered at lowest level and in between node sinkis used at middle level. This system deals with dynamic leavesand joins in mobile sensing using the timestamp of the participants.

KEYWORDS: Encryption, Multi-hop network, Mobile Sensing, Data Aggregator, Privacy

I. INTRODUCTION

The Wireless Mobile wireless sensor network can be simply definedas WSN with mobile as sensor nodes.These nodes consistof a radio transreceiver and a microcontroller powered by abattery.The topology used for these network is not decided.So,routing becomes challenging job.Data Aggregation is nothing but collection of data fromdifferent resouces or nodes and giving output as asummary.The aggregation statistics are normally computedperiodically to analyse its pattern.The source informationfor data aggregators may originate from public records anddatabases,the information is packaged into aggregate reportsand then may sold to different agencies.These reports can beused in background checks and to make some decisions.Mostof the works in this consider that the aggregator is trusted.Butthis is not the case each time.The challenge is to protectdata when the aggregator is untrusted.Many of the recentworks[2][3],consider the time series data and untrustedaggregator.In this, for the purpose of protection of data ,a new encryption scheme is introduced. In this schemes ,aggregatordecrypts only the sum of all users data instead of individualusers data.

In this paper,we propose a protocol to get sum aggregate inmulti-hop network and considering the untrusted aggregator.Incomputer networking, a hop represents one portion of thepath between source and destination.When communicatingover the internet,data passes through a number of intermediatedevices like routers rather than flowing directly over a singlewire .Each such device causes data to hop between one pointto point network connection.In this paper we consider a multihopnetwork where three levels are maintained.The lowestlevel consists of mobile nodes and in the middle level there arenode sink and at highest level there is main aggregator.Usersmay join and leave in mobile sensing networks.So in thepropose scheme dyanamic leaves and joins are maintainedwith the help of parameters like density,distance and time.Withthe help of sum aggregation.min aggregation is calculated. Innext section II we are presenting the literature survey overdifferent methods presented.

II. RELATED WORK

In the literature survey section we are going to discuss about recent methods regarding:
QinghuaLi,GuohongCao,ThomasF.LaPorta [1] introducedthe scheme that is based on the increasing capabilities ofsmart phones This scheme provides privacy to each user byobtaining Sum aggregate and Min aggregate.This scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

uses HMAC based key management technique to performefficiently.This scheme uses redundancy in security to reducecost of joins and leaves.the scheme deals with limited numberof users.

VibourRastogi and SumanNath[2] proposes the firstdifferentially private aggregation algorithms for distributed time series data with untrusted server called PASTE.PASTEfocuses on data mining applications which consist of an untrusted aggregator that is to run aggregate queries onthe data. PASTE uses two algorithms that are FourierPerturbation Algorithm (FPA) and Distributed LaplacePerturbation Algorithm (DLPA).PASTE proposes a pair of algorithms that answer queries on time-series data. FPAis used to answer long query sequences in a parallel way and DLPA implements Laplace noise addition in distributedway.In this scheme,for communication between users and aggregator ,a extra round is required which makes the schemecostly.

Elaine Shi,T-H HubretChan,Rieffel[3] introduces a systemthat maintains the privacy of each participant and considers the untrusted aggregator.In this construction,a group ofparticipants periodically uploads the data and aggregatorcomputes the sum of all data.The two important aspectsthat are focused in this construction is data randomization procedure and encryption at each participant or userwith separate key.This paper describes Private StreamAggregation(PSA) that consists of encrypted data of userthat is uploaded to aggregator.This scheme may not work for large systems or we can say multilevel systems.

Yang ,Zhong and Wright [4] proposes a cryptographicapproach that is able to maintain many customers and theirsettings and provides them privacy. In this frequencies ofvalues are computed from the customers data.It do not require any communication between customers .Each customer needs to send a single flow .This scheme becomes quite expensiveif rekeying is required and hence this scheme may not bework worthly for time series data. Shi,Y.Zhang,Liu and R.Zhang [5] proposes data aggregationscheme that uses data slicing and mixing techniques.This scheme can not be used for time-series data.The overallscheme takes long delays as it takes number of rounds between users and aggregator for communication. Theaggregation functions can be applied to this scheme but it is quite costly.

III. PROBLEM STATEMENT

The System introduces sum aggregation of time-series data in the presence of an untrusted aggregator.Based on sum aggregate,a protocol for Min aggregate is proposed.Also, the scheme deals with dynamic leaves and joins

IV. PRELIMINARIES

A. A Straw-man Construction

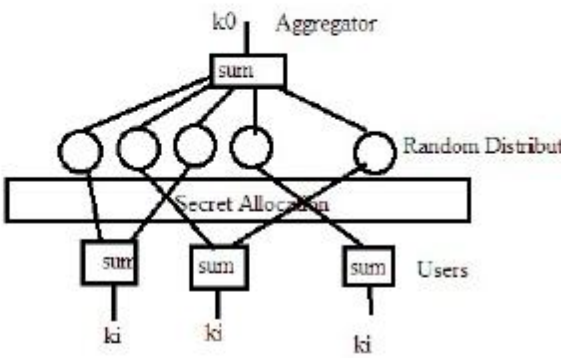

Fig. 1. Straw man Construction

Consider that there are nc random numbers.The aggregatorcalculates the sum of all these numbers and this is used as decryption key. Consider k0 as decryption key.nc Randomnumbers are divided into n users and each user is assigned with unique subset of nc.Each user calculates sum of allnumbers assigned to it and set it as encryption key.Considerki

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

as encryption key of user i. Let S denote the set of secretsand Si denotes ith subset. Lets consider that s1,s2,snc be the different secrets.
Encryption Key Generation
ki =Σh(fs(t))modM
Decryption key Generation
k0 =Σh(fs(t))modM

V. PROPOSED SYSTEM FRAMEWORK AND DESIGN

A. ARCHITECTURE

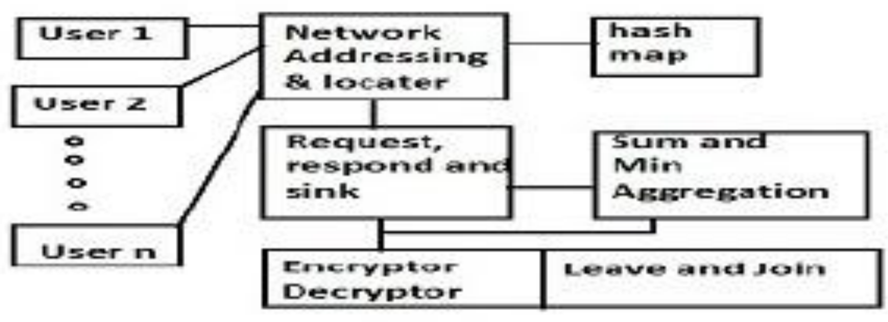

Fig.2 System Architecture

B. Network Model

In the network model, the nodes are placed inthe most bottom of the network model. The node sink isused to manage the nodes. The node sink behaveslike a cluster head of the mobile nodes. At the highest level,there is main aggregator where the actual sum and minaggregation is done. For communication between two nodes,both of them need to communicate through main aggregatorand respective node sinks. Dynamically the leaves and joinsare maintained for this network using factors like distance of each node.

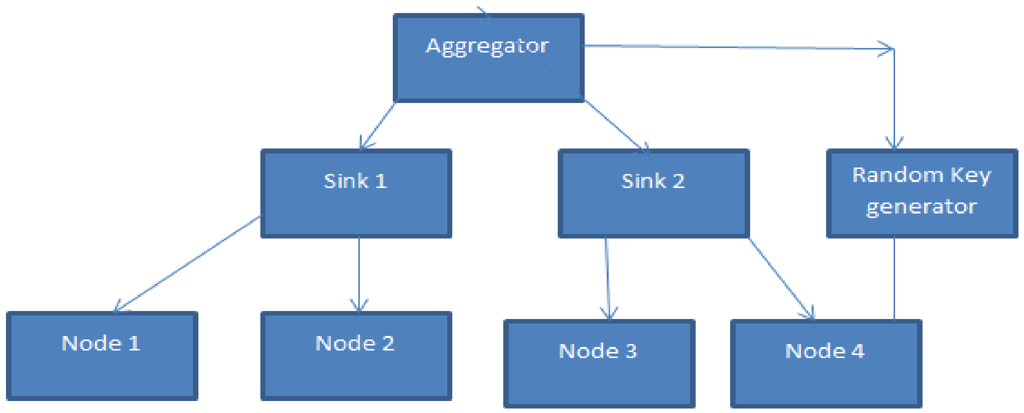

Fig 3:Network Model

The proposed algorithm for data aggregation and session key generation and each detailing of techniques are described in section 3.C.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

C. Algorithms

Algorithm 1: For Network Model

Level 1
If (S is Secure)
then, combine all sensor data
from its own region
End if
Level 2
If(S€Sn)
then, check present sessionId
if(sessionId not present)
then create new data set
End if
Level 3
If(not)
Check that data present in TDS
or not
Check if same sessionId
Else
Forward data to nearest Base
station
Entry to TDS
Session encrypt data
Add sessionId
Apply signature on it

Algorithm 2: At Main Aggregator

1. Create a server Socket.
2.Generate a PVSS engine passing the number of secrets, the threshold and the number of bits to be used.
3.Generate n secret keys (one for each party)
4.Generate n public keys using the corresponding secret keys
5.Generate the encrypted shares and their proof
6.Each party verify the received decrypted share
7.Each party extract its share with the help of min .
8.Combine the first T shares to obtain the secret back i.e the sum is caluculated.
9.Depending upon the time stamp decided prior ,the node is allowed to join or not is decided.

D. Mathematical Model

We can describe the system mathematically. Let A be theoverall system.So, A can be described asA is a set of input, output,process. So,diagrammatically thesystem can be described as:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

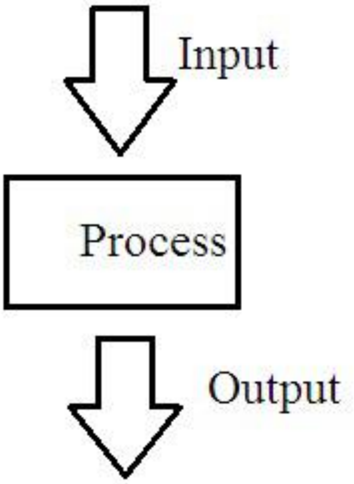

Fig.4 Illustration

Input is file containing data from source
Output is file containing data at destination more securely
Process:
1.Sum aggregation

S=S.multiply(Sh[x[i].modPow(Sh[x[i]].modPow(lambda,q)).mod q
Where
S is secret and Sh is Share generated.
2.Min aggregation
M=min(S)
3.Dynamic Leaves and Joins
t = time for communication
if t <threshold value`
then allow a node to join
if t >threshold value
then allow a node to leave.

VI. PRACTICAL RESULTS AND ENVIRONMENT

In this section we are presenting practical environment, dataset used, and metrics computed.

A. Software Used

Software Configuration
- Operating System: Windows 7
- Programming Language: Java

B. Results

Input
1. Request from sender node
2. File from one node.

Output

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

File is received at destination node with more security.

Results

	Security	No. of nodes manage	Time to receive packets	Dependencies
Previous System	Less	Less	Less	Aggregator
Proposed System	More	More	Moderate	On main aggregator and sink node

Table 1:Comparision of previous and proposed system

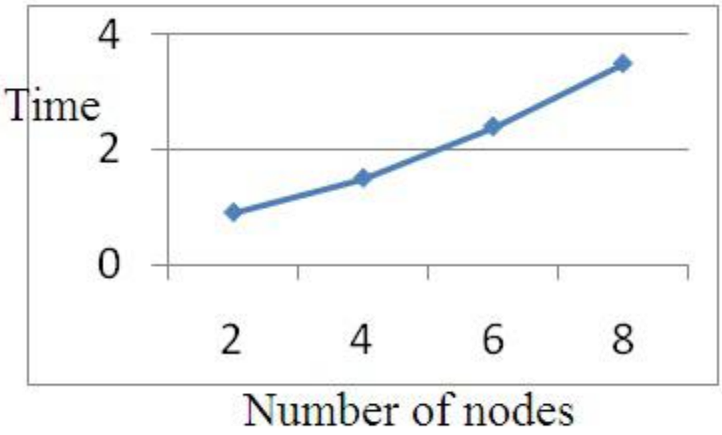

Fig 5 : Graph of proposed system

The comparision of previous and proposed system is given in Table 1.The factors like security,Number of nodes the system can manage,dependanies etc are used to compare the proposed system with previous systems.Previously,a single level containing different nodes is managed.So,there is a restriction on number of nodes the system can manage.As this is multihop system and we are maintain three levels,the more number of nodes can be managed by the system.There can be slight difference in receiving packet.At each level encryption and decryption is done.So,it may take some more time but it provides more security as compared to previous one. The graph is plotted against number of nodes and time required.As the number of nodes increased,the time will increase.

VII. CONCLUSION

This paper provides each user its own privacy withsum aggregation of individual users data.The protocol usesHMAC based key management technique to provide efficientaggregation.This protocol will handle more users thanexisting system. Based on the Sum aggregation protocol,Minaggregate is calculated.To deal with dynamic leaves and joins the factors like density,distance is considered.The main aim of this project is to introduce a secure MultisinkTime Stamp scheme. To reach this objective, the secure andoptimally efficient Straw-man type aggregated Key variant was extended to a multiparty setting to yield a MultisinkTime Stamp scheme, which provides a guaranteed traceability

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

property. The proposed Multisink Time Stamp scheme wasshown to satisfy all of the specified security requirements andfulfills the stronger break-resistant property. The MultisinkTime Stamp aggregated Key scheme thus remains secure,even if the threshold cryptosystem has been broken, i.e.,the group secret or individual secret shares are known or controlled by an adversary. The efficiency analysis showed that the proposed MultisinkTime Stamp scheme outperforms other existing schemes and is optimal in terms of exponentiations with respect tothreshold aggregated Key verification and near optimal for individual aggregated Key verification, while providing breakresistance.

ACKNOWLEDGEMENT

I would like to thank the anonymous referees for their helpful guidance that has improved the quality of this paper. Also I would like to thank my Project Guide Prof. D.N.Rewadkar, for his valuable guidance.

REFERENCES

[1] QinghuaLi,GuohongCao,Thomas F. La Porta,Efficient and Privacy-Aware Data Aggregation in Mobile Sensing, IEEE transaction on Dependable and Secure Computing, Vol. 11,No. 2,March/April 2014

[2] V. Rastogi and S. Nath, Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption, Proc. ACM SIGMOD Intl Conf. Management of Data, 2010.

[3] E. Shi, T.-H.H. Chan, E. Rieffel, R. Chow, and D. Song, Privacy Preserving Aggregation of Time-Series Data, Proc. Network and Distributed System Security Symp. (NDSS 11), 2011.

[4] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, Prisense: Privacy Preserving Data Aggregation in People-Centric Urban Sensing Systems, Proc. IEEE INFOCOM, pp. 758-766, 2010.

[5] Z. Yang, S. Zhong, and R.N. Wright, Privacy-Preserving Classification of Customer Data without Loss of Accuracy, Proc. Fifth SIAM Intl Conf.Data Mining (SDM 05), pp. 21-23, 2005.

[6] M. Jawurek and F. Kerschbaum, Fault-Tolerant Privacy- Preserving Statistics, Proc. 12th Privacy Enhancing Technologies Symp.(PETS 12), 2012.

[7] M. Shao, Y. Yang, S. Zhu, and G. Cao, Towards Statistically Strong Source Anonymity for Sensor Networks, Proc. IEEE INFOCOM, 2008.

[8] C. Castelluccia, Efficient Aggregation of Encrypted Data in Wireless Sensor Networks, Proc. Second Ann. Intl Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 05), pp. 109-117, 2005.

[9] M. Bellare, New Proofs for NMAC and HMAC: Security without Collision-Resistance, Proc. 26th Ann. Intl Conf. Advances in Cryptology (CRYPTO 06), pp. 602-619, 2006.

[10] Q. Li and G. Cao, Providing Privacy-Aware Incentives for Mobile Sensing, Proc. IEEE PerCom, 2013.

BIOGRAPHY

Asmita D. Abhyankar Post graduate student of RMDSinhgad School of Engineering, Savitribai Phule PuneUniversity. She received B.E. in Information Technologyfrom Information Technology department of Pune VidyarthiGrihas College of engineering and technology from Universityof Pune, Pune). Currently she is pursuing M.E. in Computer Engineering from RMD Sinhgad School of Engineering, Warje, Pune, Savitribai Phule Pune University.

Prof. D. N. Rewadkar received M.E. Computer Technology,from S.R.T.M. University, Nanded (2000).Currently he is working as the H.O.D of Computer Engineering Departmentin RMD SSOE,Warje, Pune. He was a Member of Board ofStudy committee of S.R.T Marathwada University, Nanded forComputer Science Engineering. He has 21 years of teachingexperience.