Key Generation using Aggregation Protocol for achieving Privacy in Mobile Sensing

[1]Johanna Edwin, [2]P.S Smitha,
[1]P.G Scholar, [2]Assistant Professor
Computer Science and Engineering
Velammal Engineering College, Anna University, Tamil Nadu, India

***Abstract* - Mobile sensing applications play a role in collecting the desired statistics from large number of mobile users. In today's world, cell phones come with multiple sensors which enable the aggregator to provide collective information. In the existing system, there is bidirectional interchange between the mobile nodes and the aggregator or high processing overhead. The communications between the untrusted aggregator and the mobile node requires high level of privacy. By generation of secret keys which are not known to each other, privacy is achieved. Key generation is implemented using sum aggregation protocol and it scales to large systems.**

***IndexTerms* - Secret keys, Sensors, Cryptosystem, Encryption, Decryption and Aggregator.**

I. INTRODUCTION

OBILE computing is a technology, which enables a computer to be transported during normal usage. This includes mobile Mhardware, mobile software and its communication. Hardware includes or device components. Nowadays mobile phones, for example, PDA's play a key role in mobile sensing applications. Mobile software includes the mobile applications' characteristics. Mobile Communication issues include communication properties and protocols. There are at least three different classes of mobile computing items:

Portable computers include a full character set keyboard and software that may be parameterized, as notepads, laptops, notebooks, etc.

Mobile phones include some restricted key set and some of them may include cell phones, smart phones, phone pads, etc.

Wearable computers are limited to functional keys and some of them may include necklaces, keyless implants, watches, wristbands etc [1].

Nowadays Mobile devices such as smart phones gain popularity and most of the smart phones are equipped with embedded sensors such as GPS, microphone, accelerometer, camera, and so on. The sensors generate data that provide information about people's health, activity and their surrounding which includes pollution, oxygen level. Thus various sensing applications are carried. Some of them include environmental monitoring, healthcare, and so on [2].

Most advanced mobile phones are furnished with a rich set of inserted sensors. This empowers different portable sensing applications, for example, ecological checking, activity checking, medicinal services etc. The mobile user sends information and it may be possible to sense private data along with the sensed data and highest priority is achieving privacy of the mobile user.

There is a need to obtain the normal sum of everyday exercises that individuals do, which might be utilized to summarize open health conditions [3] with the help of motion sensors [4]. Monitoring the normal or extreme level of air contamination [5], may help the individuals to fix their open air exercises. In numerous situations, the information from clients should be secure, and generally clients don't believe any outside aggregator to see their information values. For example, to screen the engendering of influenza, the aggregator will check the amount of clients tainted by this influenza.

Some works on data aggregation using a sensor assume a trusted aggregator. This does not protect user privacy against an untrusted aggregator in mobile sensing applications. Consider the aggregation of time-series data [9], [10], [11], [12] in the presence of an untrusted aggregator. Encryption schemes are designed to protect user privacy. On decryption, the aggregator will get only the sum of all users' data and the individual data is not known and hence user privacy is achieved. Other works which use threshold to build such an encryption scheme have some drawbacks. Decrypting the sum yields an extra round of interaction between the aggregator and all users in every aggregation period and hence resulting in high communication cost and long delay. Moreover, until decryption is performed all users need to be online, which may be highly impossible in multiple scenarios due to connectivity and user mobility.

This paper discusses about the Protocol which will obtain the sum aggregate of time series data. Key generation will be performed in which the secrets are assigned to the aggregator and to all mobile nodes. Decryption key is computed by adding all the secret keys assigned to the aggregator. The total secrets are grouped into 'n' disjoint sets and each set is given to a mobile node. The rest of the paper is organized as follows.

Section II presents discussion about System Architecture, Section III presents Related Work, Section IV presents Implementation, Section V presents Experimental Study and Section VI represents Conclusion.

II. SYSTEM ARCHITECTURE

Fig 1 shows the architecture of how the aggregator collects sensitive data from multiple mobile nodes. This architecture describes about network formation, each network consists of multiple nodes which form a region. Here we consider the nodes to be mobile nodes. And these mobile nodes are sensed by the aggregator, the key generator generates multiples keys and assigns it to the aggregator whereas the keys are subdivided and assigned to mobile nodes.

The aggregator achieves privacy because he does not know the keys given to mobile nodes and hence the mobile nodes also achieve privacy. The mobile nodes do not know the keys assigned to the aggregator. The aggregator computes aggregation statistics from the data which will be sensed from multiple nodes. The statistics may include minimum, average, etc. Then all these information will be stored in the database and can be accessed anytime.

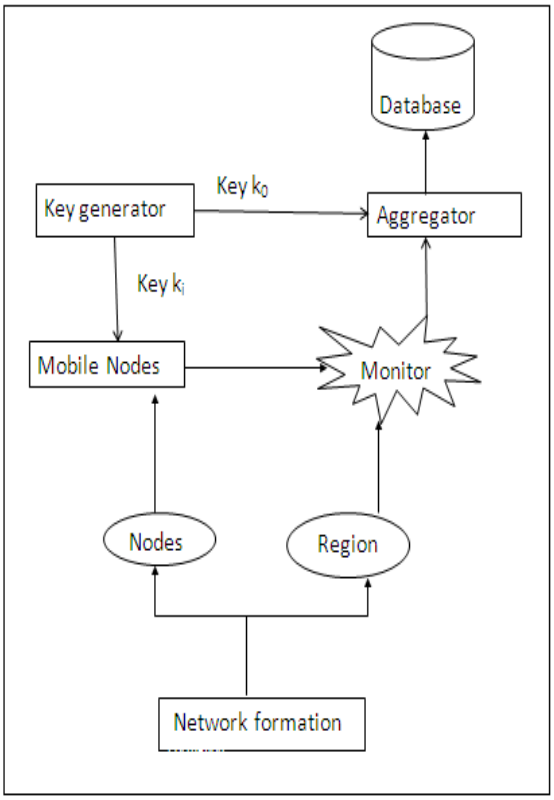

Fig 1: System Architecture

III. RELATED WORK

M.Mun et al [6] proposed Participatory Sensing Systems which generates PEIR report. The Personal Environmental Impact Report (PEIR) uses location data sampled from everyday mobile phones to calculate personalized estimates of environmental impact and exposure. Some of the location data which may be used are traffic, weather and other data. Participatory sensing is the collection of distributed data and their analysis at the personal and global scale. In this sensing, participants make key decisions on what data is being sensed, from where and when they are being sensed. The infrastructure formed by an installed base make such adaptive and mobile sensing systems. GPS data with external knowledge is being used to find about bus routes and bus stops in this method. Another important use is the prediction of user's transportation mode such as walking or taking a bus. For the PEIR application, it is most important to identify driving activities and less important to distinguish between staying and walking because emission values are zero in both cases.

J.Hicks et al [7] proposed Privacy preserving aggregation algorithms which allows a group of participants to periodically upload encrypted values to a data aggregator and the aggregator is capable of computing only the sum of all participants' values in every time period. This utilizes applied cryptographic techniques that allow the aggregator to decrypt the sum from multiple cipher texts which are encrypted under different user keys. This describes a distributed data randomization procedure which guarantees the differential privacy of the outcome statistic. This method supports only polynomial sized plaintext spaces for computing the sums. This becomes very expensive for a large system with large plaintext space.

Rastogi and Nath [8] proposed differentially private aggregation of time-series with transformation and encryption (PASTE). The aggregator, who performs the collection of cipher texts of users, multiplies them and sends the aggregate cipher text to all users. Decryption is done by each user in order to obtain a part of the sum aggregate. All the parts are collected by the aggregator and thus aggregator gets the final sum. The drawback is that it requires an extra round of interaction between the aggregator and users in every aggregation period. To answer 'n' queries, it results in a noise of O (n), when 'n' is large it is practically impossible. This Fourier Perturbation Algorithm (FPA_k) algorithm perturbs the Discrete Fourier Transform of the query answers.

For answering n queries, this method improves the expected error to O (k) by using FPA_k where 'k' is the number of Fourier coefficients that can reconstruct all the 'n' query answers. In this method, Distributed Laplace Perturbation Algorithm (DLPA) adds noise in a distributed way for guaranteeing differential privacy. Distributed differentially private algorithm can scale to a large number of users.

Shi et al [9] proposes privacy preserving stream aggregation. In this method, author considers an untrusted aggregator collects privacy sensitive data from users, and computes aggregate statistics periodically. This method achieves fault tolerance This mechanism was designed to allow an aggregator to have an accurate estimate of statistics, as well as guarantying user privacy against the untrusted aggregator. This method can efficiently support dynamic joins and leaves. In this, the main techniques for achieving failure tolerance is to build a binary interval tree over n users, and allow the aggregator to estimate the sum of contiguous intervals of users, which is represented by nodes in the interval tree.

In this paper, we implement the sensing of data from mobile nodes by an aggregator. The main objective is achieving user privacy when the user shares the sensitive information, by generating the key value pairs to the aggregator and to the mobile nodes. The values that are assigned to the nodes are not known to the aggregator and hence user privacy is achieved. Thus the aggregator can prepare a report on the sensed data from a region.

IV. IMPLEMENTATION

A. Network Topology

In our first module, we have to establish the Network. In this, network consists of 'N' nodes and region. Multiple nodes are assigned to a region. Multiple regions can be created. Based on the coverage of the region, nodes are assigned to that region. These nodes are used to communicate to each other indirectly through the region nodes. Using multicast socket, all nodes under a region can be detected. Environmental information is being monitored from all nodes in a region. Some of them are temperature, humidity.

B. Key Generation

The key generator assigns multiple secret keys to the aggregator. The aggregator has access to all the numbers and it computes the sum of these numbers as the decryption key. The computed decryption key is assigned to the aggregator who performs the computations with the sensed data.

C. Key Distribution

The secret values assigned to the aggregator are divided into disjoint subsets, each of size of the users. The aggregator cannot know any user's encryption key because it does not know the mapping between the random numbers and the users.

D. Triggering data and Aggregation

Data is being triggered from each mobile node. The data to be sensed by the aggregator is ready for data aggregation. By using the keys, data from each region is collected by the aggregator. From this collected data, aggregation is being performed by the aggregator. The aggregate is defined as the minimum value of the users' data. This scheme gets the Min aggregate of each time period and parallel Sum aggregates in the same time Period. By this aggregation, user privacy is achieved by means of generating keys to the aggregator and distributing keys to various mobile nodes.

V. EXPERIMENTAL STUDY

Experimental study includes how the mobile nodes are added into the region and how the data is sensed by the aggregator. This also studies about how privacy of every mobile user is preserved.

A. Experimental Results:

The following results have been achieved while setting up the experiment in mobile sensing using key generation.

1) Single round of interaction between the aggregator and the mobile nodes.
2) Individual user's privacy is preserved by generating and distributing the keys to multiple nodes.
3) No peer to peer communication among users.

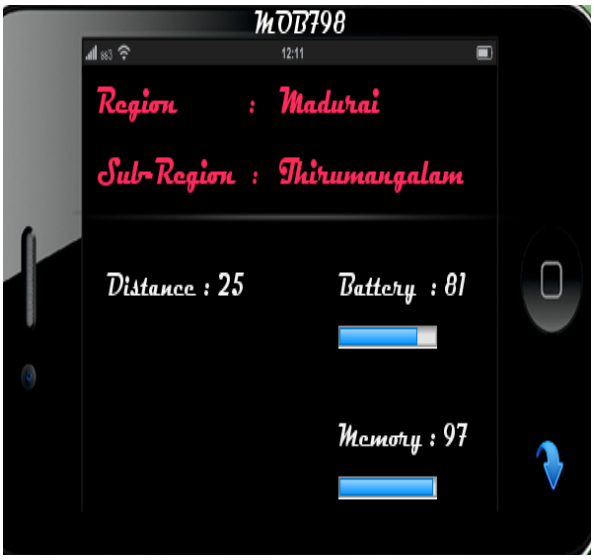

Fig 2: Mobile node generation

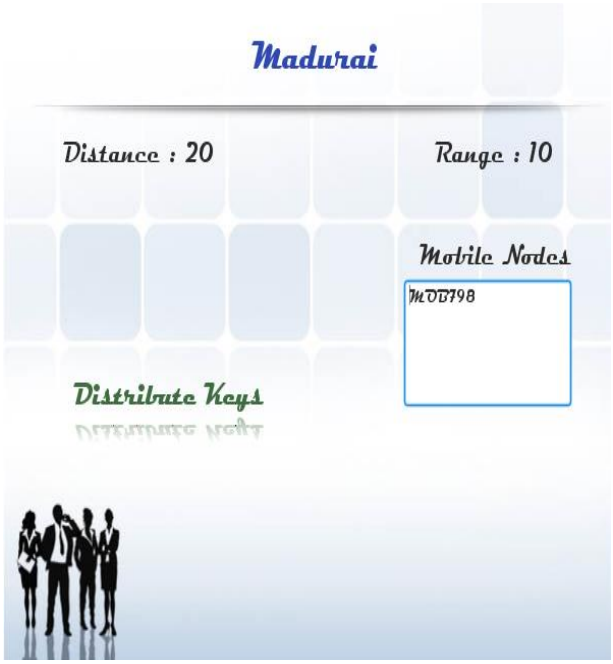

Fig 3: Addition of mobile nodes

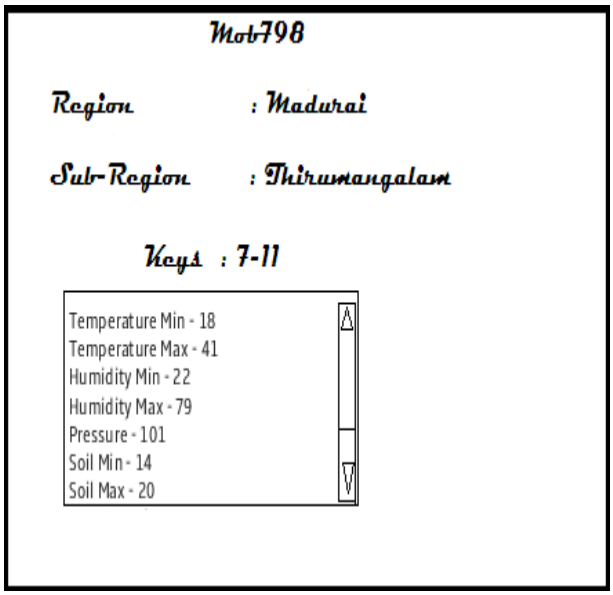

Fig 4: Sensing data from the mobile node

VI. CONCLUSION

In this paper, we have presented a detailed study on how an untrusted aggregator periodically obtains the desired statistics over the data in mobile sensing, contributed by multiple mobile users. Accumulation of data is achieved without compromising the privacy of each user. Taking into account the Sum accumulation convention, we additionally anticipated two plans to determine the Min total of time-arrangement information. One plan can acquire the correct Min, while the other one can acquire a surmised Min. To manage element joins and leaves, we presented conspire that uses the repetition in security to lessen the correspondence cost for each one join and clear out.

REFERENCES

[1] "Mobile Computing" http://en.wikipedia.org/wiki /Mobilecomputing
[2] Q. Li and G. Cao, "Efficient and Privacy Preserving Data Aggregation in Mobile Sensing," Proc. IEEE, IEEE transactions on dependable and secure computing, vol. 11, no. 2, March/April 2014.
[3] S. Consolvo, D.W. McDonald, T. Toscos, M.Y. Chen, J. Froehlich, B. Harrison, P. Klasnja, A. LaMarca, L. LeGrand, R. Libby, I.Smith, and J.A. Landay, "Activity Sensing in the Wild: A Field Trial of Ubifit Garden," Proc. SIGCHI Conf. Human Factors in Computing Systems (CHI '08), pp. 1797-1806, 2008.
[4] N.D. Lane, M. Mohammod, M. Lin, X. Yang, H. Lu, S. Ali, A.Doryab, E. Berke, T. Choudhury, and A. Campbell, "Bewell: A Smartphone Application to Monitor, Model and Promote Wellbeing," Proc. Fifth Int'l ICST Conf. Pervasive Computing Technologies for Healthcare, 2011.
[5] M.G. Apte, W.J. Fisk, and J.M. Daisey, "Indoor Carbon Dioxide Concentrations and SBS in Office Workers," Proc. Healthy Buildings Conf., pp. 133-138, 2000.
[6] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin, M.Hansen, E. Howard, R. West, and P. Boda, "Peir, the Personal Environmental Impact Report, As a Platform for Participatory Sensing Systems Research," Proc. ACM/USENIX Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '09), pp. 55-68, 2009.
[7] J. Hicks, N. Ramanathan, D. Kim, M. Monibi, J. Selsky, M. Hansen, and D. Estrin, "AndWellness: An Open Mobile System for Activity and Experience Sampling," Proc. Wireless Health, pp. 34-43, 2010.
[8] V. Rastogi and S. Nath, "Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption," Proc. ACM SIGMOD Int'l Conf. Management of Data, 2010.
[9] T.-H.H. Chan, E. Shi, and D. Song, "Privacy-Preserving Stream Aggregation with Fault Tolerance," Proc. Sixth Int'l Conf. Financial Cryptography and Data Security (FC '12), 2012.
[10] V. Rastogi and S. Nath, "Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption," Proc. ACM SIGMOD Int'l Conf. Management of Data, 2010.
[11] 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.
[12] E.G. Rieffel, J. Biehl, W. van Melle, and A.J. Lee, "Secured Histories: Computing Group Statistics on Encrypted Data While Preserving Individual Privacy,"http:// arxiv.org /abs /1012 .2152, 2010.