Survey on Secured Multi Sink Data Aggregation Scheme in Mobile Sensing

Tejashree Borbande[1], Vikas Maral[2]

[1]P.G. Scholar, Dept. of Computer Engineering., KJ's COE Management & Research, Savitribai Phule University of Pune, India

[2]Professor, Dept. of Computer Engineering., KJ's COE Management & Research, Savitribai Phule University of Pune, India

Abstract: ***Smart Mobile phones especially are getting more and more importance in day to day life. These mobile phones are now facilitated with number of applications that are using sensors such as camera, microphone, GPS, accelerometer, ambient light sensor, gyroscope, and so on. With the help of large numbers of individual participants, aggregation which is computed from data is really useful and helps to predict the statistics of Result. Aggregation guarantees more privacy of the data from individual participants. This paper provides a solution for preserving the individual participants privacy by using aggregate function like Sum, Min. Calculation of Sum aggregation is done without releasing the participant's information. Min aggregation is calculated using Sum aggregation. Min aggregation is nothing but minimum value of data. In this paper, a multi-hop network is considered where, there is a main aggregator at the highest level and mobile nodes are considered at lowest level and in between node sink are used at middle level. This system deals with dynamic leaves and joins in mobile sensing using the timestamp of the participants.***

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

1. Introduction

The Wireless Mobile wireless sensor network can be simply defined as WSN with mobile as sensor nodes. These nodes Consist of a radio Trans receiver and a microcontroller powered by battery. The topology used for this network is not decided. So, routing becomes challenging job. Data Aggregation is nothing but collection of data from different resources or nodes and giving output as a summary. The aggregation statistics are normally computed periodically to analyses its pattern. The source information for data aggregators may originate from public records and databases, the information is packaged into aggregate report sand then may sold to different agencies. These reports can be used in background checks and to make some decisions. Most of the works in this consider that the aggregator is trusted. But this is not the case each time. The challenge is to protect data when the aggregator is untrusted. Many of the recent works[2][3],consider the time series data and untrusted aggregator. In this, for the purpose of protection of data ,a new encryption scheme is introduced. In this schemes ,aggregator decrypts only the sum of all users data instead of individual users data pick before observe the equivalent keyword search trapdoors. It seems an suitable security concept, particularly if the keyword space has no high min-entropy.

In this paper, we propose a protocol to get sum aggregate in multi-hop network and considering the untrusted aggregator. In computer networking, a hop represents one portion of the path between source and destination. When Communicating over the internet, data passes through a number of intermediate devices like routers rather than flowing directly over a single wire .Each such device causes data to hop between one point to point network connections. In this paper we consider a multihop network where three levels are maintained. The lowest level consists of mobile nodes and in the middle level there are node sink and at highest level there is main aggregator. Users may join and leave in mobile sensing networks. So in the propose scheme dynamic leaves and joins are maintained with the help of parameters like density, distance and time. With the help of sum aggregation. min aggregation is calculated

2. Literature Survey

We propose the first differentially private aggregation algorithm for distributed time-series data that offers good practical utility without any trusted server [2]. This addresses two important challenges in participatory data-mining applications where (i) individual users wish to publish temporally correlated time-series data (such as location traces, web history, personal health data), and (ii) an untrusted third-party aggregator wishes to run aggregate queries on the data. To ensure differential privacy for time-series data despite the presence of temporal correlation, we propose the Fourier Perturbation Algorithm (FPA). Standard differential privacy techniques perform poorly for time-series data. To answer n queries, such techniques can result in a noise of Theta (n) to each query answer, making the answers practically useless if n is large. Our FPA algorithm perturbs the Discrete Fourier Transform of the query answers. For answering n queries, FPA improves the expected error from Theta (n) to roughly Theta (k) where k is the number of Fourier coefficients that can (approximately) reconstruct all the n query answers. Our experiments show that $k << n$ for many real-life data-sets resulting in a huge error-improvement for FPA. [2] To deal with the absence of a trusted central server, we propose the Distributed Laplace Perturbation Algorithm (DLPA) to add noise in a distributed way in order to guarantee differential privacy. To the best of our knowledge, DLPA is the first distributed differentially private algorithm that can scale with a large number of users: DLPA outperforms the only other distributed solution for differential privacy proposed so far, by reducing the computational load per user from O(U) to O(1) where U is the number of users.[2]

We consider how an untrusted data aggregator can learn desired statistics over multiple participants' data, without compromising each individual's privacy. [3] We propose a construction that allows a group of participants to periodically upload encrypted values to a data aggregator, such that the aggregator is able to compute the sum of all participants ' values in every time period, but is unable to learn anything else. We achieve strong privacy guarantees using two main techniques. First, we show how to utilize applied cryptographic techniques to allow the aggregator to decrypt the sum from multiple ciphertexts encrypted under different user keys. Second, we describe a distributed data randomization procedure that guarantees the differential privacy of the outcome statistic, even when a subset of participants might be compromised.

We consider applications where an untrusted aggregator would like to collect privacy sensitive data from users, and compute aggregate statistics periodically. For example, imagine a smart grid operator who wishes to aggregate the total power consumption of a neighborhood every ten minutes; or a market researcher who wishes to track the fraction of population watching ESPN on an hourly basis. We design novel mechanisms that allow an aggregator to accurately estimate such statistics, while offering provable guarantees of user privacy against the untrusted aggregator. Our constructions are resilient to user failure and compromise, and can efficiently support dynamic joins and leaves. Our constructions also exemplify the clear advantage of combining applied cryptography and differential privacy techniques.

Several public key cryptosystems with additional homomorphic properties have been proposed so far. They allow performing computation with encrypted data without the knowledge of any secret information In many applications, the ability to perform decryption, i.e. the knowledge of the secret key, gives a huge power.[6] A classical way to reduce the trust in such a secret owner, and consequently to increase the security, is to share the secret between many entities in such a way that cooperation between them is necessary to decrypt. In this paper, we propose a distributed version of the Paillier cryptosystem presented at Eurocrypt '99. This shared scheme can for example be used in an electronic voting scheme or in a lottery where a random number related to the winning ticket has to be jointly chosen by all participants.

3. Existing System

- Sensor data aggregation assumes a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications. Several recent works consider the aggregation of time-series data in the presence of an untrusted aggregator. To protect user privacy, they design encryption schemes in which the aggregator can only decrypt the sum of all users' data but nothing else.
- Use threshold Paillier cryptosystem to build such an encryption scheme. To decrypt the sum, their scheme needs an extra round of interaction between the aggregator and all users in every aggregation period, which means high communication cost and long delay. Moreover, it requires all users to be online until decryption is completed, which may not be practical in many mobile sensing scenarios due to user mobility and the heterogeneity of user connectivity.

Disadvantages of Existing System:
- Cannot protect user privacy against untrusted aggregators.
- Existing works do not consider the Min of time-series data

4. System Architecture

In the network model, the nodes are placed in the most bottom of the network model. The node sink issued to manage the nodes. The node sink behaves like a cluster head of the mobile nodes. At the highest level, there is main aggregator where the actual sum and min aggregation is done. For communication between two nodes, both of them need to communicate through main aggregator and respective node sinks.

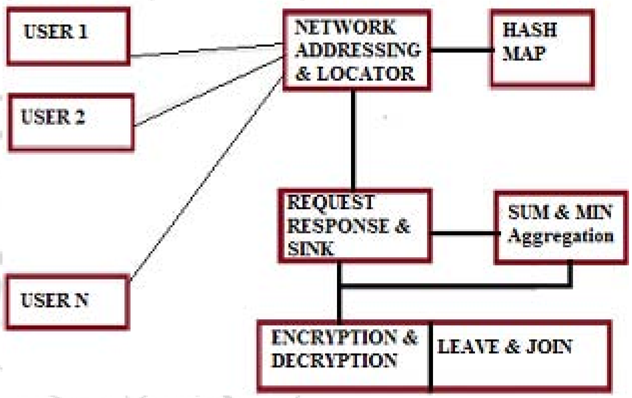

Figure 1: System Architeture.

Modules

- System Model Module
- Encryption Scheme Module
- Key Generation Module
- Aggregation Protocol Module

5. Modules Description

System Model Module
In this module first we develop our system model, with mobile users. An aggregator wishes to get the aggregate statistics of n mobile users periodically, for example, in every hour. The time periods are numbered as 1, 2, 3, . . . , and so on. In every time period, each user i encrypts her data xi with key ki and sends the derived ciphertext to the aggregator. From the ciphertexts, the aggregator decrypts the needed aggregate statistics using her aggregator capability k0. In each time period, a mobile user sends her encrypted data to the aggregator via WiFi, 3G or other available access networks. No peer-to-peer communication is required among

mobile users, since such communication is nontrivial in mobile sensing scenarios due to the high mobility of users and users may not be aware of each other for privacy reasons. We consider an untrusted aggregator that is curious about each individual user's data. The aggregator may eavesdrop all the messages sent from/to every user. A number of users may collude with the aggregator, and reveal their data to the aggregator. A number of users may also collude to obtain the aggregate.

Encryption Scheme Module

One building block of our solution is the additive homomorphic encryption scheme. Encryption is the process of translating plain text data (*plaintext*) into something that appears to be random and meaningless (*ciphertext*). Decryption is the process of converting ciphertext back to plaintext. To encrypt more than a small amount of data, *symmetric encryption* is used. A *symmetric key* is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.

The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key. It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks.

Key Generation Module

Suppose there are nc random numbers. The aggregator has access to all the numbers, and it computes the sum of these numbers as the decryption key k0. These numbers are divided into n random disjoint subsets, each of size c. These n subsets are assigned to the n users, where each user has access to one subset of numbers. User i computes the sum of

the numbers assigned to it as the encryption key ki. The aggregator cannot know any user's encryption key because it does not know the mapping between the random numbers and the users. When c is large enough, it is infeasible for the aggregator to guess the numbers assigned to a particular user with a brute-force method. The aggregator's decryption key cannot be revealed by any user because no user knows all the numbers.

Aggregation Protocol Module

The Min aggregate is defined as the minimum value of the users' data. This module presents a protocol that employs the Sum aggregate to get Min. Each user uses just one set of secrets for all instances of the sum aggregation protocol.When the plaintext space is large, the cost of the basic scheme is high. In some application scenarios, it may not be necessary to get the exact Min, but an approximate answer is good enough. For such scenarios, the basic scheme can be extended to get an approximate Min with much smaller cost.

6. Conclusion

This paper provides each user its own privacy with sum aggregation of individual user's data. The protocol uses HMAC based key management technique to provide efficient aggregation. This protocol will handle more users than existing system. Based on the Sum aggregation protocol, Min aggregate 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 Multi sink Time Stamp Scheme. To reach this objective, the secure and optimally efficient Straw-man type aggregated Key variant was extended to a multiparty setting to yield a Multi sink Time Stamp scheme, which provides a guaranteed traceability property. The proposed Multi sink Time Stamp scheme was shown to satisfy all of the specified security requirements and fulfills the stronger break-resistant property. The Multilink Time 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 Multisink Time Stamp scheme outperforms other existing schemes and is optimal in terms of exponentiations with respect to threshold aggregated Key verification and near optimal for individual aggregated Key verification, while providing break resistance.

7. 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. V.M.Maral ,** 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, Sharing Decryption in the Context of Voting or Lotteries, 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 NFOCOM, 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.
[11] MNDOLI, “Mnosha Permissible Exposure Limits,” http:// www.dli.mn.gov/OSHA/PDF/pels.pdf, 2013.
[12] S.B. Eisenman, E. Miluzzo, N.D. Lane, R.A. Peterson, G.-S. Ahn, and A.T. Campbell, “The Bikenet Mobile Sensing System for Cyclist Experience Mapping,” Proc. ACM Fifth Int’l Conf. Embedded Networked Sensor Systems (SenSys ’07), pp. 87-101, 2007.
[13] 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.
[14] Z. Zhu and G. Cao, “APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-Based Services,” Proc. IEEE INFOCOM, 2011.
[15] Q. Li and G. Cao, “Mitigating Routing Misbehavior in Disruption Tolerant Networks,” IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.
[16] E.D. Cristofaro and C. Soriente, “Short Paper: Pepsi—Privacy- Enhanced Participatory Sensing Infrastructure,” Proc. Fourth ACM Conf. Wireless Network Security (WiSec ’11), pp. 23-28, 2011.
[17] Q. Li, S. Zhu, and G. Cao, “Routing in Socially Selfish Delay Tolerant Networks,” Proc. IEEE INFOCOM, pp. 1-9, 2010.
[18] Q. Li, W. Gao, S. Zhu, and G. Cao, “A Routing Protocol for Socially Selfish Delay Tolerant Networks,” Ad Hoc Networks, vol. 10, no. 8, pp. 664-675, 2012.
[19] D. Bonet, E.-J. Goh, and K. Nissim, “Evaluating 2-DNF Formulas on Ciphertexts,” Proc. Second Int’l Conf. Theory of Cryptography (TCC ’05), 2005.
[20] ket Telephone, Inc.

Author Profile

Tejashree V. Borbande, Post graduate student of **KJCOEMR, Pune,** Savitribai Phule Pune University. She received B.E. in Information Technology from Pune University. Currently she is pursuing M.E. in Computer Engineering from **KJCOEMR , Pune,** Pune, Savitribai Phule Pune University.

Prof. V.M.Maral Working as Asst. Professor in Computer Engineering Department of KJ’s Collegeof Engineering Management and Reasearch, Pune