IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Fault-Tolerant Preserving Statistics Encrypted Data Aggregation in WSN

A.Krishnaveni , S.Rajiya sulthana

CSE,BCETW,KADAPA , AP, INDIA

CSE,BCETW,KADAPA , AP, INDIA

ABSTRACT

Mobile devices such as smart phones are gaining an ever-increasing popularity. Most smart phones are equipped with a rich set of embedded sensors such as camera,microphone,GPS, accelerometer, and so on. in many scenarios, users are privacy-sensitive, and users do not trust any single third-party aggregator to see their data values. A user may not want to directly provide her true status Thus, an important challenge is how to protect the users' privacy in mobile sensing, especially when the aggregator is untrusted. To protect user privacy, they design encryption schemes in which the aggregator can only decrypt the sum of all users data but nothing else. 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. we propose a new protocol for mobile sensing to obtain the sum aggregate of time-series data in the presence of an untrusted aggregator. Our protocol employs an additive homomorphic encryption and a novel key management scheme based on efficient HMAC..

KeyWords: additive homomorphic, novel key management,data aggregation,dataencryption,mobile sensing

1.Introduction

Most previous works on sensor data aggregation assume a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications.

In this paper, we propose a new protocol for mobile sensing to obtain the sum aggregate of time-series data in the presence of an untrusted aggregator.

2.Existing system

Sensor data aggregation assumes a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications.

To protect user privacy, they design encryption schemes in which the aggregator can only decrypt the sum of all users' data but nothing else.

2.1 Proposed System

We propose a new privacy-preserving protocol to obtain the Sum aggregate of time-series data.

The protocol utilizes additive homomorphic encryption and a novel, HMAC-based key management technique toperform extremely efficient aggregation.

3. Tables,Figures and Equations

3.1 Tables and Figures

Security in the Straw-Man Construction

n	10^2	10^3	10^4	10^5	10^6
$\gamma = 0, 0.1, 0.2, 0.3$	11	8	6	5	4

Table 1 The Minimum Values of c for 80-bit Security in the Straw-ManConstruction

ISSN 2348 – 7968

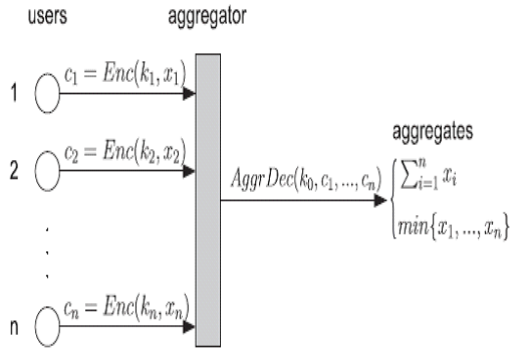

Fig1.Our system model of time-series data aggregation.

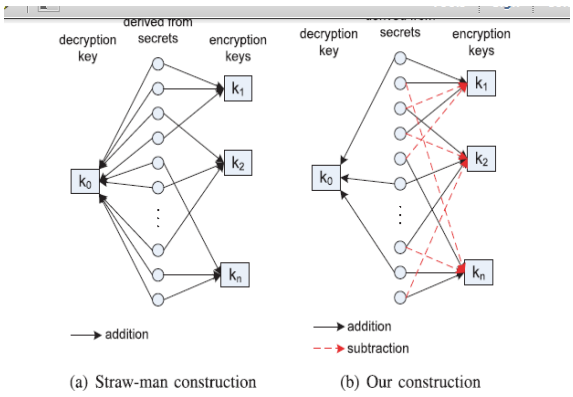

Fig. 2 The intuition behind our construction in comparison with thestraw-man construction.

3.2 Equations

Consider an equation:

a1 + a2 + …… + anc= ¼ a1 + a2 +….+anc

If we remove nc - q summands from the right side and subtract them from the left side, the derived equation

a1 + ….+anc + (_a1) +….+ (-anc-q)= anc-q+1 +….+ anc.

4. Conclusion

Based on the Sum aggregation protocol, we also proposed two schemes to derive the Min aggregate of time -series data.

To deal with dynamic joins and leaves, we proposed ascheme that utilizes the redundancy in security to reduce the communication cost for each join and leave.

Acknowledgments

The authors would like to thank the anonymous reviewers fortheir insightful comments. A preliminary version of this paper appeared in IEEE ICNP 2012.This work was supported in part by the Army Research Office under MURI grantW911NF-07-1-0318.

References

1.J. Shi, R. Zhang, Y. Liu, and Y. Zhang, Proc. IEEE INFOCOM, pp. 758-766, 2010

2.D.Bonet, E.-J. Goh, and K. Nissim,Proc. Second Int'l Conf. Theory of Cryptography(TCC '05), 2005.

3. M. Jawurek and F. Kerschbaum, Proc. 12th Privacy Enhancing TechnologiesSymp. (PETS '12), 2012.

First Author: A.krishnaveni completed Btech in 2013 under jntua with first class with distination and also attended national and international conferences.

SecondAuthors:S.Rajiyasultana completed mtech in 2013 under the jntuh with distination and publish several international journels and also attended national and international conferences.