ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

PRIVACY-AWARE DATA AGGREGATION MECHANISM FOR MOBILE SENSORS USING ENHANCED CDAMA

B.Sharmila[1], Mrs.Sandhiya.P[2]

[1]M.E.Scholar, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India

[1]sharmilabanu.38@gmail.com,[2]sandhiya.p@nandhaengg.org

Abstract:

Data aggregation is needed to be statistical framework between number of mobile users and aggregator. The homomorphic encryption applies for hidden communication during aggregation time period, ensures that enciphered data can be aggregated algebraically without decryption. Aggregators can collect the data without decryption, but it is unsecured in the scheme of multiple applications environment. Although there are some presented works in this area that required two way communication between the aggregator and mobile users. So, the concealed data aggregation scheme extended from BGN homomorphic public encryption system. For multi-application environment, CDAMA performs data aggregation in multiple groups for secure communication and it has three contributions. First, the multiple-applications environment is designed. Second, the single application WSN is intended for adversaries. Third, provides secure counting capability. Finally, the unauthorized aggregations are damaged. Furthermore, the CDAMA applied in database service environment. The result illustrate CDAMA scheme to increase high- level security.

Keywords: WSN, Mobile Sensing, Data Aggregation, Homomorphic Encryption.

1. Introduction

Wireless sensor networks are composed works of nodes where each node has its own sensor, processor, transmitter, receiver, sensors usually low cost devices that perform a specific type of sensing task. Due to low cost of sensors that deploy intimately throughout the particular area to monitor specific situation that have been occur. The wireless sensor networks typically work in public and unrestrained area; so the security is a major challenge in sensor applications. Hence the resource constraints in the sensor nodes, traditional security mechanism with large operating cost of computation and communication are infeasible in WSNs. Based upon the security requirements and protocols to provide regimented data transmission between parties. The sensor networks actively monitor their surroundings and security is handled in hostile environment. The security is most important in wireless sensor network context between two network entities should provide requirements confidentiality, authentication, Integrity. Thus, security in wireless sensor network plays an imperative role in the security of the whole network and review is made that how to provide the security on wireless sensor networks.

For mobile access networks, different technologies have been developed Wi-Fi is technology for wireless LANs and tiny range transmission from source to destination. Also, WiMAX is technology for last mile broadband connection; Wireless USB is technology for Internet connectivity.

Prolong with, mobile sensing applications such as smart phones ever increasing popularity in recent trend. As though, mobile device easily monitor environmental conditions, traffic monitoring, health care [3] and so on. Depending on the purpose of each application, sensor node adapted to read different kinds of data (e.g., light, smoke and thermometer).

In mobile sensing applications, [1] to sense the data by using smart phones and composed data send it to the aggregator. Finally, the aggregator forward the aggregation results to the sink node or base station i.e. BS.

Statistical data [2] can be sporadically obtain the desired over contribute by multiple mobile users that is termed as data aggregation. The intercession of unauthorized aggregation obtained the desired statistical data of time period. So, our protocol sum aggregate which it employs an additive homomorphic encryption and key management scheme based on efficient MAC to ensure that the aggregator can only acquire the sum of all user data, without knowing individual user's data or intermediate result.

Each user and aggregator only needs to compute the encrypted data and decrypt the sum of all user data. Therefore, computation cost is very low and the protocol supports large plaintext spaces, high aggregation loads.

Consequently, Min-time series data and Max value obtained during mobile sensing. The calculations are derived by many other statistics such as count, max and average. Since the users may frequently join and leave in mobile sensing, the CDAMA performs the data aggregation between multiple groups and it employs redundancies for security to reduce the communication cost to deal with dynamic join s and leaves.

2. Data Aggregation

Aggregation stats necessitate to be sporadically computed from a flow of data contribute by mobile users [3], are very useful. The statistical data from users are seclusion-sensitive, and users do not belief any single third-party gathering aggregator to see their data values. Accordingly, systems that accumulate users' true data values and computed.

Sensor data aggregation assumed a trust aggregator, and hence cannot protect user solitude against an unfrosted aggregator in mobile sensing applications. To protect user seclusion, they design encryption schemes in which the aggregator can only decrypt the sum of user's data but nothing else.

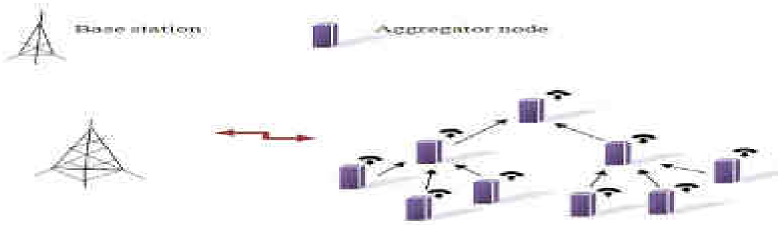

Figure 3.1 Data Aggregation

To decrypt the sum, their scheme needs a second round of interaction between the aggregator and users in every aggregation era, which means high communication cost and long delay. Furthermore, none of these presented schemes considers the Min time-sequence data which is also important in many mobile sensing applications.

3. Theoretical Analysis

Theoretically, there are two preserving privacy of users proposed methods for contributing location privacy-aware data aggregation for mobile sensors. The first Sum Aggregate Protocol is extended and Homomorphism encryption, MAC-ECC based the public key cryptography algebraic operations are performed.

One building block of the solution is the additive homomorphism encryption scheme under Sum aggregate protocol work:

Encryption: Represent message m as an integer within range [0, M-1], where M is a large integer. Let k be a randomly generated key. Output cipher text c (m + h(f_kr))) mod M, where f_k is a pseudorandom function (PRF) that uses k as a parameter, h is a hash function and r is the sample value for the message.

Decryption: Output plaintext m = (c - h(f_kr))) mod M.

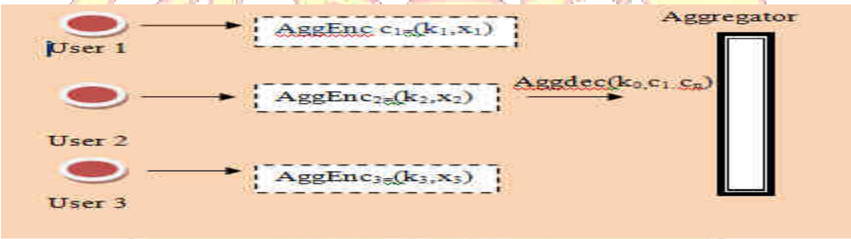
User 1
User 2
User 3
AggEnc c_1=(k_1,x_1)
AggEncc_2=(k_2,x_2)
AggEncc_3=(k_3,x_3)
Aggdec(k_0,c_1.c_n)
Aggregator

Figure 4.1 Basic Encryption Scheme

3.1 Key generation for Sum Aggregate and Min Aggregate

Setup: The key dealers assign a set of surreptitious values to each user and the aggregator.

Encry: In each time period, user generate encryption key ki using the surreptitious that it is assigned. It sends the cipher text ci to the aggregator.

AggreDec: In each time period, the aggregator generates decryption key k0 using the secrets that it is assigned, and decrypts the sum aggregate.

The Min aggregate is defined as the minimum value of the users' statistical data. In each time era, each user generates Δ + 1derivative data d [0], d [1] .., d [Δ] where each imitative data match to one possible data value in the plaintext space.

Likewise, Max aggregate Protocol performed. Differential seclusion provides strong privacy guarantee for users such that a user's contribution in the system only leak trifling information about the user. Our protocol for Sum can be adapted to provide computational differential privacy.

3.2 MAC – ECC

Based on Elliptic Curve Cryptography, considered for multiple groups for generate the message authentication code between one toward another node. Then, next hop transmissions is sustained represented the curve as rounded circle and the number of sensor nodes deployed in that oval circle. The sensor nodes continuously sense the data and collected and with local distance capability to virtually coordinated by using public-key cryptography. Following that the sensed data are aggregated and aggregated data send to the Aggregator. Consequently, forward the aggregation results to Base station.

4. Cdama

4.1 Aggregator Model

New - fangled Concealed Data Aggregation Scheme (CDAMA) scheme protocol for mobile sense to obtain the sum aggregate of time-series data in the presence of an unfrosted aggregator and also used for secure communication between one node and two groups of nodes. The homomorphism encryption public key based system to communicate surreptitious aggregation between multiple groups in multiple applications.

The concealed data aggregation scheme extended from BGN homomorphic public encryption system. For WSN environment, CDAMA performs data aggregation in multiple groups for secure communication and it has three contributions.

First, the multiple-applications WSN environment is designed. Second, the single application WSN is intended for adversaries. Third, provides secure counting capability. Finally, the unauthorized aggregations are damaged.

The data aggregation support algebraic operations and utilizes the privacy homomorphism encryption to assist aggregation in encrypted data. The CDAMA scheme designed for multiple application WSNs.

In practice, SN having different purposes, e.g., In Biosensors intended for biomedical Electronics detected MRI, CT, X Ray, ECG, Heart Sound, Temperature, Blood Pressure, Image Processing, Signal Processing and delivering Light, Current, Heat, Ultrasound.

The Figure 4.1 explains about to distribute the keys for each users with the help of key dealer assign by aggregator. For each users are sensed the data and to assign the key to encrypt the statistical or numerical data and send it to the aggregator.

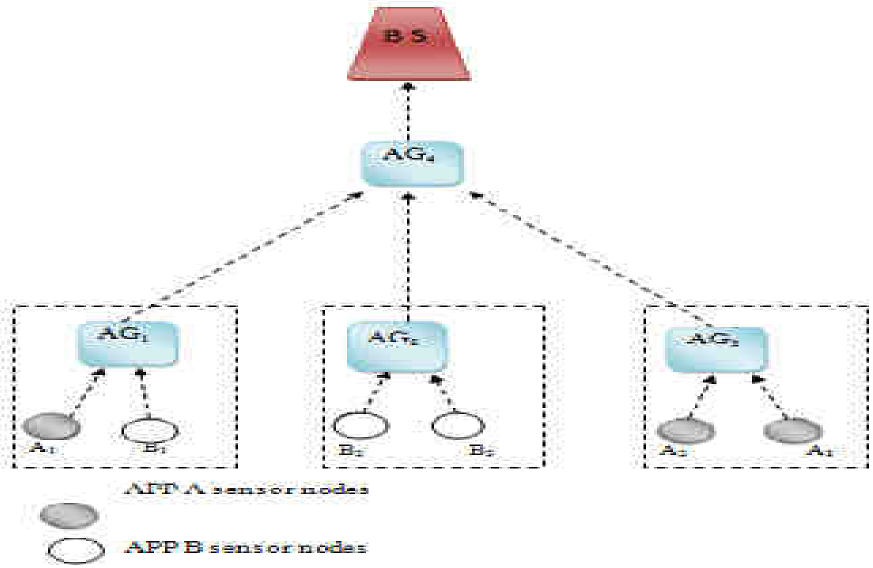

Figure 4.1 Key Distribution for multiple applications

Underneath, BGN scheme is performed to generating the key between the mobile users and the aggregator by using prime numbers give stronger security and better applicability in CDA support ahead all over MAC-ECC and Homomorphism encryption.

4.2 Privacy homomorphic Cryptosystem

The privacy homomorphic encryption is an encryption scheme for imply that algebraic operations on plaintexts can be executed by manipulating the multiple cipher texts. For example, Enc(m_1) and Enc(m_2) into $D_K(E_K(m_1) \circ E_K(m_2))$ =m1+m2, where E_K is an encrypt the data with key K, D_K is an decrypt the data with key K. The operation + and · multiplication and addition denoted to obtain the cipher texts and plain texts respectively.

Typically, PH schemes are categorized into two ways. Symmetric cryptosystem used for encrypt the data and decrypt the data by using same key or asymmetric cryptosystem (also called public key cryptography) when two keys are different. MAC-Elliptic curve cryptography intention to generate the authentication code linking from one node to another node for secure communication subsequently next hop transmissions sustained. Homomorphism encryption has been useful to secrete communication through aggregation such that enciphered data can be aggregate arithmetically without decryption. Since aggregators bring together data without decryption, adversaries are not capable to falsify aggregated results by compromising them.

The benefit of proposal that employs the idleness in security to reduce the communication cost of dealing with dynamic join and leaves and further each time era, a mobile user sends her encrypted data to the aggregator via Wi-Fi or available access networks.

Besides, CDAMA scheme for a multi-application environment, which is the first scheme. Through CDAMA, the cipher texts from distinctive applications can be aggregated, but not varied. For a sole-application environment, CDAMA is still safer than other CDA schemes. Secure communication between two groups of nodes which have lower communication operating cost. As well, the CDAMA method applied in network environment and also applied in database service environment. The goal guaranteed the privacy of each user's data against the unfrosted aggregator.

5. Conclusion

For WSN environment, CDAMA performs data aggregation in multiple groups for secure communication. By generating the MAC-ECC used for sending the message and receiving the message between the mobile users and aggregator. Through CDAMA scheme, three scenarios are applied. First, the multiple-applications WSN environment is designed for aggregating the cipher texts of different applications separately. Second, the single application WSN is intended for adversaries. Third, base station exactly knows the number of messages aggregated due to the secure counting capability. Finally, the unauthorized aggregations are damage by CDAMA scheme. Moreover, the CDAMA is applied in database service environment and also to realize aggregation query in Database-As-a-Service (DAS) model. In DAS model, a client stores their database on an unfrosted service provider. Hence, CDAMA scheme predict efficiency and robustness.

References

[1]. QInghua li, Member, IEEE, Guohong Cao, fellow, IEEE, AND Thomas F. La Porta, Fellow(2014), IEEE "Efficient and Privacy-aware Dataaggregation in Mobile Sensing" Ieee Transactions On Dependable And Secure Computing, VOL. 11, NO. 2.

[2]. John Hicks, Nithya Ramanathan, Donnie Kim, Mohamad Monibi, Joshua Selsky, Mark Hansen And Deborah Estrin. (2014) "Andwellness: An Open Mobile System For Activity And Experience Sampling."Proc Wireless Health, Pp.34.Vol.10, No.3.

[3]. Elaine Shit-H. Hubert Chane Eeanor Rreffel (2011), "Privacy-Preserving Aggregation Of Time- Series Data ", Ieee Proc. Network And Distributed System Security Symp, Vol. 12, No. 3.

[4]. T-H. Hubert Chan ,Elaine Shi Dawn Song (2012),"Privacy-Preserving Stream Aggregation With Fault Tolerance", Proc.Sixth Int'l Conf.Financial Cryptography And Data Security.Vol.15.No.1

[5]. Daojing He, Mohsen Guizani,(2015)," Accountable And Privacy-Enhanced Access Control In Wireless Sensor Networks "Ieee Transactions On Wireless Communications", Vol. 14, No. 1.

[6]. Jian Li, Yun Li, Jian Ren, Senior Member, Ieee, And Jie Wu, Fellow(2014),"Hop-By-Hop Message Authentication And Source Privacy In Wireless Sensor Networks" ,Ieee Transactions On Parallel And Distributed Systems, Vol. 25, No. 5.

[7]. Qinghua Li ,Guohong Cao,(2014), "Providing Privacy-Aware Incentives For Mobile Sensing" ,Ieee Transactions Vol 4,Issue 4.

[8]. Huang Lu,Jie Li,Mohsen Guizani (2014) , "Secure And Efficient Data Transmission For Cluster-Based Wireless Sensor Networks", Ieee Transactions On Parallel And Distributed Systems Vol 25,N0.3.

[9]. A.Thiagarajan, (2009),"Accurate, Energy-Aware Road Traffic Delay Estimation Using Mobilephones," Proc. Acm Seventh Conf. Embedded Networked Sensorsystems (Sensys '09), Pp. 85-98.

[10]. N.D. Lane, And A. Campbell (2011),"Bewell: Smartphone Application To Monitor, Model And Promote Wellbeing," Proc. Fifth Int'l Icst Conf. Pervasive Computing Technologies For Healthcare.

[11]. V. Rastogi And S. Nath, (2010), "Differentially Private Aggregation Of Distributed Time-Series With Transformation And Encryption," Proc. Acm Sigmod Int'l Conf. Management Of Data.

[12]. C. Castelluccia, And G. Tsudik,(2009), "Efficient And Provably Secure Aggregation Of Encrypted Data In Wireless Sensor Networks," Acm Trans. Sensor Networks, Vol. 5,No. 3, Pp. 20:1-20:36.

[13] Junbcom Hur,Kyungtae Kang (2014)" Secure Data Retrieval For Decentralized Disruption-Tolerant Militiary Networks" Ieee Acm Transactions On Networking Vol:4,No.2.

[14] Reza Soosahabi, Mort Naraghi-Pour(2014) "Optimal Probabilistic Encryption For Secure Detection In Wireless Sensor Networks Protocol Design", Ieee Transactions On Information Forensics And Security, Vol. 9,3.